La seguridad no es un juego

Seguridad para Gamers

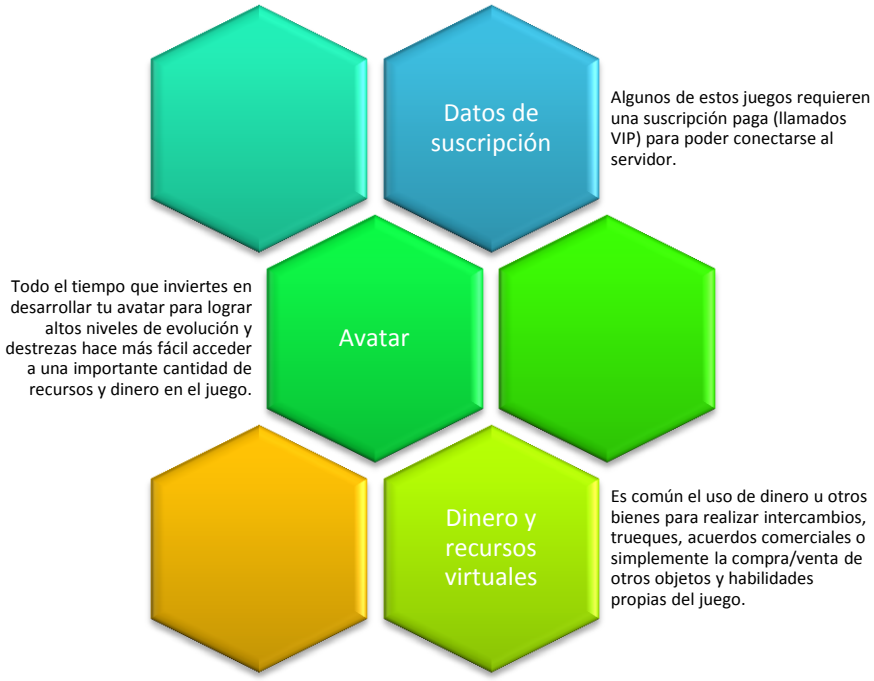
ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Índice

¿Qué tan vulnerable crees que puedes ser?

Quizá muchos piensan que al estar inmersos en su juego no están expuestos a ataques de códigos maliciosos o que puedan llegar a ser víctimas de alguna estafa. Lo cierto es que alrededor de toda la industria de los juegos se mueve tanto dinero que ha hecho que los creadores de malware posen sus ojos en este tipo de plataformas, ya que manipulando los recursos de los jugadores, se puede controlar el acceso al dinero real invertido en el mundo virtual.

Ahora la pregunta que puede surgir es: ¿Qué se pueden robar en un mundo virtual?



En otras palabras, el uso de tarjetas de crédito para pagar por suscripciones y otros servicios, sumado a que un usuario puede convertirse virtualmente en “millonario” es el punto de partida para que exista un campo de acción para los códigos maliciosos.

¿Por qué un gamer es atractivo para los ciberdelincuentes?

Quienes pasan muchas horas envueltos en la dinámica de un videojuego no dimensionan que pueden estar expuestos a riesgos, quizá pensando que el hecho de no utilizar los recursos de su computadora como un usuario convencional lo haría, no lo expone a riesgos. A continuación mencionamos las características que convierten a un *gamer* en una potencial víctima para los ciberdelincuentes.

Métodos para robar información

Aunque el comportamiento de un *gamer* es diferente al de un usuario corriente, comparten vulnerabilidades por las cuáles les podrían robar su información, además aparecen unas no tan corrientes que por sus particularidades los pueden afectar.

La obtención de esta información tiene como objetivo, a los juegos más populares y extendidos, sin embargo, las similitudes entre los distintos títulos, las formas de registro y los datos necesarios para

jugar hacen que el malware ya existente pueda ser modificado fácilmente para adaptarse a otro juego si fuera necesario, dando lugar a diferentes variantes.

¿Dónde están los riesgos?

Por la forma en que un *gamer* utiliza los recursos de su computadora y dados las exigencias en recursos de los juegos, hay una serie de comportamientos característicos que ponen en riesgo la seguridad de su información.

Análisis de casos reales de códigos maliciosos

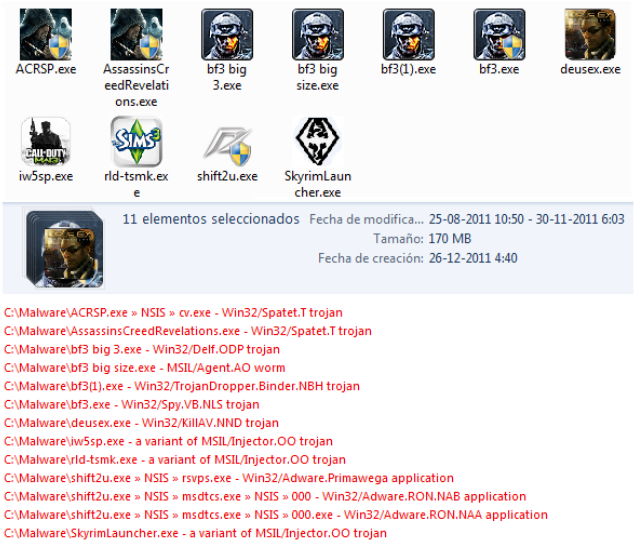
Como se pudo observar en el documento, los atacantes desarrollan y adaptan ataques informáticos como códigos maliciosos, phishing y tácticas de Ingeniería Social específicamente para usuarios de videojuegos. A continuación se detallan algunos casos diseñados para robarle información a este tipo de usuarios:

Códigos maliciosos e Ingeniería Social

Archivos infectados de gran tamaño para engañar a gamers

Existen varios códigos maliciosos que son propagados por los cibercriminales utilizando temáticas de Ingeniería Social destinadas a usuarios de videojuegos. Estas técnicas son implementadas tanto

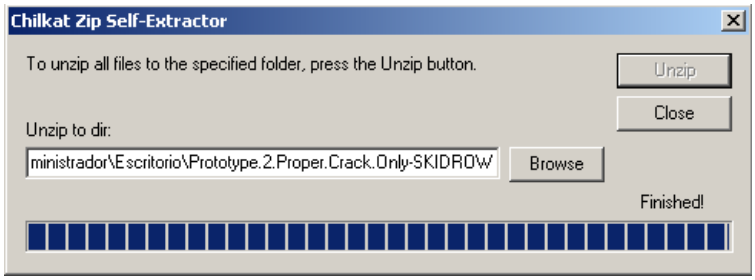
a nivel de campaña de propagación como en el código malicioso en sí. Por ejemplo, ESET Latinoamérica detectó múltiples amenazas que no solo fueron propagadas como supuestos *cracks* para juegos, sino también el tamaño de los archivos fueron aumentados intencionalmente para no despertar la suspicacia de un *gamer* que podría dudar si un fichero posee un tamaño muy pequeño para ser un *crack*. En la siguiente imagen es posible observar algunos títulos como Battlefield 3, Los Sims 3, Assassin's Creed Revelations, entre otros, siendo utilizados por ciberdelincuentes para propagar *malware* que utiliza iconos y tamaños afines:



Más información puede ser consultada en el post Archivos de gran tamaño como técnicas de ingeniería social.

***Win32/TrojanDropper.VB.OFV**: crack malicioso para Prototype 2*

Se trata de un troyano que simula ser un *crack* para un conocido videojuego, Prototype 2. Una vez que el usuario ejecuta este código malicioso, se le muestra una ventana en la que deberá especificar una ruta que se utilizará para copiar los archivos ilegítimos del juego. Lo que no visualiza la víctima es que en conjunto con la instalación del *crack*, se copia otro código malicioso (*Win32/Miner.NAB*) que ocupará los recursos de la computadora del usuario con diversos fines maliciosos. En la siguiente captura es posible visualizar la interfaz gráfica de esta amenaza en caso que sea ejecutada:



Más información puede ser consultada en el post Malware afecta a usuarios de videojuego Prototype 2.

Win32/Ainslot: *Falso crack de Crysis 3*

El falso crack de Crysis 3 viene en el interior de un ZIP o RAR cuyo nombre suele ser "Crysis 3 crack" o similar. Dentro del archivo comprimido es posible encontrar tanto el ejecutable malicioso como un fichero de texto que muestra las supuestas instrucciones y la descripción del juego. A continuación, se muestra una captura del icono utilizado en las cuatro variantes de malware analizadas en este post. Destaca el uso de un icono de alta resolución para engañar a la potencial víctima:

Los falsos cracks han sido desarrollados como archivos de gran tamaño que van desde los 7 MB hasta los 33 MB. Es probable que esto se deba a que, frente a un supuesto archivo de bajo peso, algunas personas sospecharían que se trata de algo malicioso o falso. También a los fines de sumar credibilidad al engaño, el icono de la amenaza es otro aspecto que los atacantes suelen considerar a la hora de propagar programas falsos. En este caso, los iconos son idénticos a los del ejecutable del juego original. En otras oportunidades, incluso recurren a la creación de uno nuevo en base al diseño del videojuego. Por otro lado, muchas de estas amenazas muestran al momento de ejecutarse, errores falsos que le informan al usuario que el juego no ha podido ser "*crackeado"* o incluso, copian el *crack* "funcional" mientras realizan acciones maliciosas.

Más información puede ser consultada en el post sobre el falso crack de Crysis 3 que propaga malware.

Más familias de malware que afectan a gamers

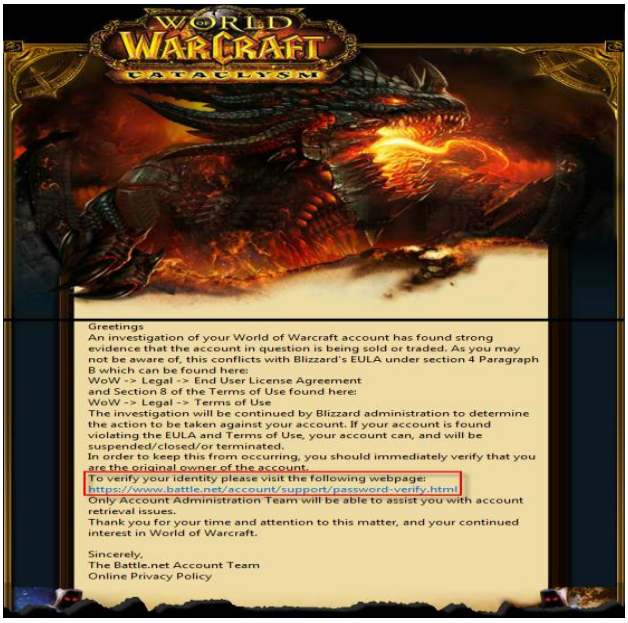
Las familias Win32/OnLineGames, Win32/PSW.WOW y otras, están diseñadas específicamente para atacar a usuarios de videojuegos en línea. El objetivo de estas amenazas es obtener las credenciales de estos juegos y en ciertos casos, la licencia de uso. Asimismo, algunos de estos *códigos maliciosos* son capaces de interceptar las cuentas de correo de las víctimas con el objetivo de buscar algún mensaje relacionado al juego y que pudiera contener información de interés para el atacante. Más información puede ser consultada en el post Juegos online en la mira.

Phishing

El phishing es una técnica que consiste en robarle información sensible a la víctima. A través de un correo electrónico o mensaje, los atacantes solicitan credenciales o datos relacionados a entidades bancarias, tarjetas de crédito, juegos en línea, etc. A continuación se muestra un caso de phishing que afecta a usuarios de un conocido juego de rol.

World of Warcraft

Este ataque llega a través de un correo electrónico que intenta asustar al usuario informándole que su cuenta de World of Warcraft ha estado involucrada en supuestas actividades que atentan en contra de las políticas del servicio. La siguiente captura muestra el mensaje:



Tal como puede verse, el texto insta a la potencial víctima a visitar un enlace con la excusa que si no lo hace, su cuenta será desactivada permanentemente. Si se sigue dicho enlace, se accede a un

sitio malicioso que solicita nombre de usuario, contraseña, y pregunta y respuesta secreta. La siguiente captura muestra la página fraudulenta:

De ingresarse esta información, los cibercriminales podrán robar la cuenta del jugador. Más información puede ser consultada en el post World of Warcraft: la batalla continúa fuera del juego.

Algunas recomendaciones

Existen una serie de consejos que se pueden seguir y que lo van ayudar a mantener a salvo la información de los juegos:

- Aunque lo más común suele ser comunicarse por voz con otros usuarios durante el juego para no perder tiempo valioso escribiendo, cuando se utiliza el modo texto lo mejor es restringir la información que se comparte en estos chats.
- El nombre de usuario dentro del juego suele reflejar una descripción del jugador. A pesar de que algunas personas utilizan nombre camuflado con L337 (Leet), lo recomendable es evitar el uso del nombre real, e incluso abstenerse de subir una foto verdadera.
- Es mucho mejor utilizar sitios oficiales para comprar los juegos online, o sino buscar tiendas virtuales reconocidas que brinden garantía en la transacción.
- 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 instalan otras aplicaciones maliciosas.

- 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.
- Buscar nuevos juegos, demos, etc., para descargar es la mejor forma de incrementar la experiencia en el juego, sin embargo, es necesario tener cuidado de dónde se hacen las descargas.
- Tener instaladas las últimas versiones de los recursos utilizados por los juegos, además de mejorar la calidad del juego, se cierran las puertas a errores de diseño y otras vulnerabilidades que pueden ser la entrada a un código malicioso o atacante.
- No desactivar la solución de seguridad mientras juegas es la mejor forma de mantener la protección contra ataques. Para esto es necesario configurarlo para lograr un mejor rendimiento.
- Descargar actualizaciones y parches para el juego de sitios oficiales, de esta forma se evitan modificaciones maliciosas del sistema.
- Preferentemente jugar en servidores oficiales. Además, normalmente estos permiten partidas privadas sin problemas.

Acerca de ESET

Fundada en 1992, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas. La empresa cuenta con oficinas centrales en Bratislava, Eslovaquia y oficinas de coordinación regional en San Diego, Estados Unidos; Buenos Aires, Argentina y Singapur. También posee sedes en Londres (Reino Unido), Praga (República Checa), Cracovia (Polonia), San Pablo (Brasil) y Distrito Federal (México).

Además de su producto estrella ESET NOD32 Antivirus, desde el 2007 la compañía ofrece ESET Smart Security, la solución unificada que integra la multipremiada protección proactiva del primero con un firewall y anti-spam. Las soluciones de ESET ofrecen a los clientes corporativos el mayor retorno de la inversión (ROI) de la industria como resultado de una alta tasa de productividad, velocidad de exploración y un uso mínimo de los recursos.

Desde el 2004, ESET opera para la región de América Latina en Buenos Aires, Argentina, donde dispone de un equipo de profesionales capacitados para responder a las demandas del mercado en forma concisa e inmediata y un laboratorio de investigación focalizado en el descubrimiento proactivo de variadas amenazas informáticas.

La importancia de complementar la protección brindada por tecnología líder en detección proactiva de amenazas con una navegación y uso responsable del equipo, junto con el interés de fomentar la concientización de los usuarios en materia de seguridad informática, convierten a las campañas educativas en el pilar de la identidad corporativa de ESET, cuya Gira Antivirus ya ha adquirido renombre propio.

Para más información, visite www.eset-la.com