LITORALPRESS

Fecha: 08-07-2025
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: Los ataques digitales a videojugadores han aumentado 55% durante el último año

Pág. : 8
Cm2: 634,0

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Varias empresas de ciberseguridad han detectado un alza en este sector:

Los ataques digitales a videojugadores han aumentado 55% durante el último año

Títulos como "Grand Theft Auto", "Minecraft" o "Call of Duty" son los más usados para engañar a las víctimas. Los delincuentes buscan apoderarse de los "tesoros digitales" de los usuarios, pero también acceder a sus cuentas bancarias.

ALEXIS IBARRA O.

Los ciberdelincuentes van hacia donde hay dinero. Y los videojuegos se han vuelto un buen botín. Millones de jugadores en el mundo están comprando títulos en línea de forma digital, y adquiriendo "objetos" para sus juegos, como armas, vestimentas o nuevos superpoderes. En los videojuegos estos inicialmente son gratuitos, pero hay que pagar si se quiere "avanzar rápido" y sin tanto esfuerzo.

En su último reporte de videojuegos y ciberamenazas, la empresa de ciberseguridad Kaspersky detectó más de 19 millones de intentos de ataques contra videojuegos populares entre jóvenes dentro del período que va entre abril de 2024 y marzo de 2025. El número de ataques mensuales aumentó un 55% entre el inicio y el final del período analizado.

Los videojuegos más atacados por los ciberdelincuentes incluyen "Grand Theft Auto", con 4.456.499 intentos de ataques, seguido de "Minecraft" con 4.112.493 y "Call of Duty" con 2.635.330 intentos.

Otros títulos usados para los ataques son "The Sims" con 2.416.443 intentos, "Roblox" con 1.548.929 y "FIFA" con 909.174.

Check Point, otra empresa de ciberseguridad, también ha detectado engaños, en específico, en "Minecraft", juego que disfrutan cerca de 200 millones de usuarios activos en el mundo. Acá el engaño es a través de *mods*, pequeños programas que modifican el juego original para añadir nuevas etapas o características. Los usuarios los instalan y no son detectados por la mayoría de los antivirus.

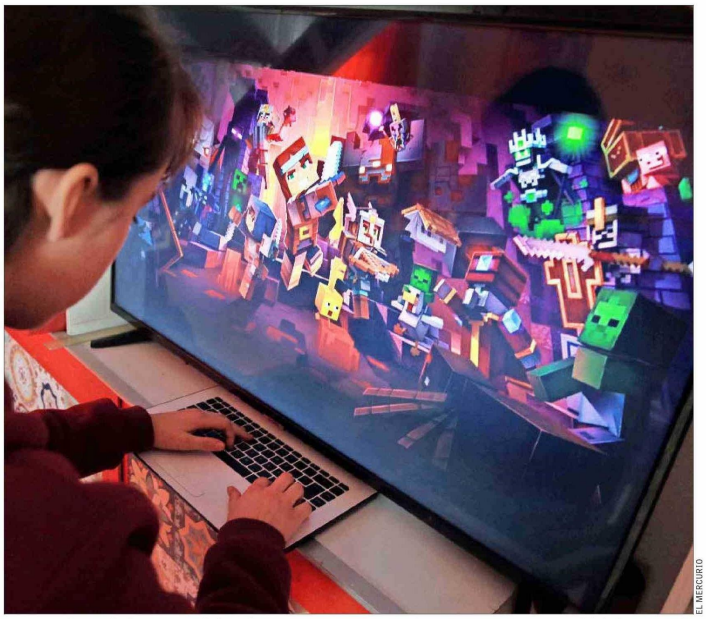
En este caso, el código malicioso que se instala en el computador roba las contraseñas de Discord (usado por los videojugadores para comunicarse), Telegram o la cuenta misma de "Minecraft". Incluso busca si en el computador hay monederos digitales con criptomonedas.

Jaromir Horejsi, especialista en inteligencia de amenazas, ingeniería inversa y análisis de *malware* de Check Point, dice que "no se sabe el número exacto de cuántos jugadores podrían haber sido infectados, pero sí que los ataques van en aumento. Además, hemos detectado cientos de variantes del ataque desde principios de este año".

Según Leandro Cuozzo, analista de Seguridad en el Equipo Global de Investigación y Análisis para A. Latina en Kaspersky, los ciberdelincuentes usan distintas técnicas para atacar.

"Uno de ellos es ofrecer a las posibles víctimas un adelanto gratuito de videojuegos de moda, incluso antes del lanzamiento", dice Cuozzo. Una variante de esa técnica es ofrecerles participar en un torneo de videojuegos con un atractivo premio.

"Pero cuando quieren acceder (al videojuego o a la invitación) reciben un enlace falso en el cual le piden a la víctima iniciar sesión en una de sus cuentas de videojuegos. Al ingresar su *login* y contraseña, la cuenta es secuestrada", agrega.



EL MERCURIO

"Minecraft", en la foto, es uno de los videojuegos que más intentos de ataques registra. Una modalidad es invitando al usuario a descargar un *mod*, modificación que agrega nuevos elementos al juego original.

Además, añade, se le puede pedir a la víctima que descargue un archivo, que en realidad es un código malicioso y que realiza acciones nocivas, como capturar todo lo que el usuario escriba en su teclado (*keyloggers*), *software* espía (*spyware*) o programas que muestran publicidad (*adware*).

Otra forma de engaño, dice Cuozzo, es enganchar a la víctima con la posibilidad de obtener objetos dentro del juego: monedas virtuales, *skins* (que permiten cambiar el aspecto del videojuego o de personajes) y cuentas mejoradas a bajo precio. Al comprar, explica, se corre el riesgo de que el ciberdelincuente se quede con el dinero pactado (si pide transferencia) o con los datos bancarios (si es que se solicita tarjeta).

Desde ESET, otra empresa de ciberseguridad, también han visto un aumento en los ataques a videojugadores. Uno de estos engaños populares es la ingeniería social: "El atacante simula ser una figura de autoridad —como el soporte del videojuego— y le pide sus credenciales (usuario y contraseña) o que ingrese a un sitio malicioso que le solicitará ingresar datos financieros o de la cuenta", dice Martina López, investigadora de Seguridad Informática de ESET Latinoamérica.

¿Por qué ha crecido esta forma de engaño? Según López, los ciberdelincuentes se han dado cuenta de que los videojugadores son generalmente jóvenes y eso los haría "más susceptibles a caer en engaños o no pensar antes de hacer clic". Otra razón que da la especialista es que suelen tener activos digitales (mejoras de personajes, monedas virtuales y otros ítems que cuestan dinero real) y que aquello tiene interés para los delincuentes, ya que pueden transar con ellos o incluso cobrar rescate al propio jugador para recuperarlos.

Como medidas de precaución los especialistas recomiendan ser precavidos ante ofertas tentadoras, comunicaciones con desconocidos o llamadas de soporte no solicitadas. Además, llaman a no descargar videojuegos desde servidores que no son los oficiales ya que pueden tener código malicioso. Y al comprar, usar tarjetas virtuales con un cupo limitado.

Película F1 es usada para robar

"F1: The Movie", la película inspirada en la Fórmula 1, ha generado una ola de actividad fraudulenta en Latinoamérica, según Kaspersky. Los estafadores atraen a las víctimas con ofertas para ver la película gratis, pero para entregar el enlace se solicita compartir información bancaria, la que es usada por los criminales para robar.

Otro gancho son los falsos sorteos de juguetes de autos de carrera relacionados con una promoción de restaurantes de comida rápida. En este caso solicitan la información de la tarjeta para supuestos gastos de envío.