Publicado en Madrid el 22/09/2022

Atención, gamers: credenciales y tarjetas de crédito, en el punto de mira

En el primer semestre de 2022, los expertos de Kaspersky detectaron un aumento de la actividad de los ciberdelincuentes que se aprovechan de los datos de los gamers. El número de usuarios atacados por software malicioso, que recopila datos sensibles y se propaga bajo la apariencia de algunos de los juegos más populares, aumentó un 13% en comparación con la primera mitad de 2021

Para evaluar el panorama actual de los riesgos de en el gaming, los expertos de Kaspersky analizaron las amenazas más populares relacionadas con los juegos para PC y móviles. En total, entre el 1 de julio de 2021 y el 30 de junio de 2022, las soluciones de seguridad de Kaspersky detectaron más de 384.000 usuarios afectados por casi 92.000 archivos únicos maliciosos o no deseados que imitaban 28 juegos o series de juegos. Además del gran número de descargadores capaces de instalar otros programas no deseados y adware, los analistas de Kaspersky detectaron incluso troyanos-espías, una categoría de software espía capaz de rastrear cualquier dato introducido en el teclado y realizar capturas de pantalla.

La investigación también reveló un crecimiento de los ataques realizados con software malicioso que roba datos sensibles de los dispositivos infectados. Entre ellos se encuentran Trojan-PSW, que recoge las credenciales de las víctimas, Trojan-Banker, que roba datos de pago, y Trojan-GameThief, que recoge información de acceso a cuentas de juego. Desde el 1 de julio de 2021 hasta el 30 de junio de 2022, las soluciones de seguridad de Kaspersky detectaron un total de 3.705 archivos únicos que distribuían este software malicioso bajo la apariencia de juegos populares o series de juegos. En el primer semestre de 2022, los investigadores de Kaspersky observaron un aumento del 13% en el número de usuarios atacados con él en comparación con el primer semestre de 2021. El número de estos archivos únicos utilizados para infectar a los usuarios también aumentó en la primera mitad de 2022 en casi una cuarta parte, en comparación con el mismo periodo de 2021: 1.868 y 1.530 archivos, respectivamente.

La mayoría de las veces, los usuarios reciben archivos maliciosos cuando intentan descargar juegos no desde sitios oficiales, sino desde webs de terceros. Esto es especialmente frecuente si un juego nuevo es bastante caro y el jugador quiere ahorrar dinero encontrando una copia gratuita en sitios poco fiables. Sin embargo, perderán mucho más que si hubieran comprado una versión legítima. Por ejemplo, muchos archivos maliciosos roban la información de acceso a las cuentas de juego, los datos bancarios e incluso los datos de las criptocarteras al infectar los dispositivos.

Los atacantes tratan de propagar las amenazas bajo la apariencia de juegos que tienen un gran público o que han sido lanzados recientemente y están constantemente en los radares de los gamers. Juegos tan conocidos como Roblox, FIFA o Minecraft, por ejemplo, así como las nuevas partes de grandes series de juegos, lanzadas durante el último año - Elden Ring, Halo y Resident Evil - fueron objeto de abuso activo por parte de los atacantes que propagaron el malware RedLine bajo su apariencia.

RedLine es un software de robo de contraseñas que extrae datos confidenciales del dispositivo de la víctima, como contraseñas, datos guardados de tarjetas bancarias, carteras de criptomonedas y credenciales de servicios VPN. Desde el 1 de julio de 2021 hasta el 30 de junio de 2022, las soluciones de Kaspersky han detectado 2.362 usuarios únicos atacados con RedLine, difundido bajo la apariencia de juegos populares, lo que la convierte en la familia de amenazas más activa durante el periodo indicado. RedLine suele venderse a un precio muy bajo en diversos foros de hackers, por lo que goza de una enorme popularidad entre los ciberdelincuentes

Además de difundir archivos maliciosos, los atacantes siguen creando y difundiendo activamente nuevas webs de phishing en el ámbito de los juegos. Por primera vez, los expertos de Kaspersky han descubierto un nuevo esquema de phishers que atacan a los jugadores. Imitando toda la interfaz de las tiendas del juego para CS:GO, PUBG y Warface, los estafadores crean webs fraudulentas, ofreciendo a las víctimas potenciales un arsenal decente de varias armas y artefactos de forma gratuita. Para recibir el regalo, los jugadores tienen que introducir los datos de acceso de sus cuentas de redes sociales, como Facebook o Twitter. Tras hacerse con las cuentas, es probable que los atacantes busquen en los mensajes personales los datos de las tarjetas o pidan dinero a varios amigos de la víctima, aprovechando su confianza y descuido.

"La pandemia impulsó la industria del juego, aumentando considerablemente el número de aficionados al juego. Los ciberdelincuentes están abusando de esta tendencia, creando cada vez más nuevos esquemas y herramientas para atacar a los jugadores y robar los datos de sus tarjetas de crédito e incluso las cuentas de los juegos, que pueden contener costosas skins que luego pueden ser vendidas. Habrá nuevos tipos de ataques a los jugadores en el próximo año. Por ejemplo, ataques a los e-sports, que ahora están ganando una enorme popularidad en todo el mundo. Por eso es tan importante estar siempre protegido, para no perder dinero, credenciales y cuenta de juego", comenta Anton V. Ivanov, investigador principal de seguridad de Kaspersky.

Para garantizar la protección mientras se juega, Kaspersky recomienda:

Es más seguro descargar los juegos sólo de tiendas oficiales como Steam, Apple App Store, Google Play o Amazon Appstore. Los juegos de estos mercados no son 100% seguros, pero al menos son revisados por los representantes de las tiendas y hay algún tipo de sistema de control: no todas las aplicaciones pueden entrar en estas tiendas.

Si se compra un juego que no está disponible en las principales tiendas, se debe adquirir sólo en el sitio web oficial. Comprobar dos veces la URL del sitio web y asegurarse de que es auténtica.

Tener cuidado con las campañas de phishing y con los jugadores desconocidos. No abrir los enlaces recibidos por correo electrónico o en un chat de juego a menos que confíes en el remitente. No abrir los archivos que recibas de desconocidos.

No descargar software pirata ni ningún otro contenido ilegal, aunque redirijan a él desde un sitio web legítimo.

Una solución de seguridad sólida y fiable será de gran ayuda, sobre todo si no ralentiza ordenador mientras juegas, pero al mismo tiempo protege de todas las posibles ciberamenazas. Por ejemplo, Kaspersky Total Security funciona sin problemas con Steam y otros servicios de juegos.

Utilizar una solución de seguridad sólida para protegerte del software malicioso y de su actividad en los dispositivos móviles, como Kaspersky Internet Security para Android.

Datos de contacto:
Mónica Iglesias
690196537

Nota de prensa publicada en: Madrid

Categorías: Nacional Juegos Software Ciberseguridad Gaming