

Roban 36 millones de contraseñas de juegos y servicios de inteligencia artificial en el mundo

El malware Infostealers infecta a los dispositivos personales y corporativos a través de correos electrónicos o sitios web suplantados

Aproximadamente 34 millones de datos de acceso al popular juego Roblox y unas 664,000 credenciales de usuarios de OpenAI, fueron expuestas en la dark web. (Kaspersky)

Hay alerta por el robo de más de 36 millones de contraseñas asociadas a juegos y servicios de inteligencia artificial que dejaron en evidencia la vulnerabilidad de los dispositivos personales y corporativos en el mundo ante ataques cibernéticos.

La operación fue especialmente significativa en plataformas como Roblox y OpenAI, incluido el popular chatbot ChatGPT. La infiltración estuvo a cargo del malware conocido como infostealers, un programa malicioso diseñado para robar inicios de sesión y contraseñas de usuarios al infectar dispositivos personales y corporativos mediante phishing y otros métodos.

Cómo Infostealers generó los ataques

Un glosario de tecnología para conocer todo lo necesario sobre este campo - (Imagen Ilustrativa Infobae)

El informe, que fue presentado en el contexto del Mobile World Congress 2024, y arrojó luz sobre el crecimiento alarmante en el número de credenciales comprometidas en los últimos tres años. En particular, el informe destaca que casi 34 millones de credenciales de Roblox, un juego muy popular entre los niños, fueron robadas y publicadas en la dark web.

La situación es especialmente preocupante cuando se trata de plataformas populares entre los menores, porque los niños se convierten en un blanco fácil para los ciberdelincuentes que utilizan técnicas de ingeniería social para engañar a los usuarios más jóvenes.

“La razón por la que se producen tantos robos de credenciales de inicio de sesión asociadas a Roblox es que los niños se encuentran entre el público más vulnerable”, explicó Yuliya Novikova, responsable del Kaspersky Digital Footprint Intelligence, subrayando la sofisticación y el peligro de estas amenazas.

Este análisis, realizado en vísperas del Mobile World Congress 2024, revela la magnitud del problema que enfrentan usuarios y empresas. (Imagen Ilustrativa Infobae)

Además, se experimentó un incremento exponencial en el robo de datos de usuarios de OpenAI en 2023, con un total aproximado de 664,000 registros comprometidos en comparación con el año anterior. Mientras que otros servicios como Canva y Grammarly, también fueron blanco de estas actividades ilícitas, con millones de inicios de sesión y contraseñas filtrados en plataformas clandestinas.

“Las credenciales en cuestión provienen de la actividad de los infostealers, una forma especializada de malware diseñada para robar contraseñas de usuarios para ciberataques, ventas en la dark web u otras actividades maliciosas”, afirmó Novikova.

Recomendaciones los expertos

18/07/2022 Applus+ Adquiere Jtsec, Empresa Española De Ciberseguridad POLITICA Europa Press

Los investigadores subrayan la importancia de implementar soluciones de ciberseguridad robustas para contrarrestar el riesgo creciente que representa el comercio de credenciales robadas en la dark web.

La especialista Novikova resaltó cómo el malware infostealer no solo se limita a afectar a los individuos a nivel personal, sino que también representa una amenaza significativa para la seguridad corporativa. “La importancia de contar con soluciones sólidas para protegerse de los ataques de los infostealers y otros programas maliciosos es cada vez mayor tanto para particulares como para empresas”, afirmó.

Y para evitar las amenazas relacionadas con las pérdidas de contraseñas, los expertos recomiendan:

- En una empresa, organizar una supervisión proactiva para identificar las cuentas comprometidas antes de que afecten a la ciberseguridad de clientes y empleados.
- En el caso de los particulares, es importante proteger todos los dispositivos que se utilicen con una solución de seguridad de confianza.
- Utilizar una contraseña diferente para cada servicio. Así, aunque los ciberdelincuentes roben una de las cuentas, no afectará al resto.
- Siempre que sea posible, hay que proteger las cuentas con autenticación de dos factores. Si no, es clave revisar la configuración de las cuentas.

Con casi 34 millones de cuentas comprometidas publicadas en la dark web entre 2021 y 2023, los niños se convierten en un blanco fácil para los ciberdelincuentes. (Poppet07)

La demanda de cuentas comprometidas, especialmente aquellas relacionadas con servicios de IA, evidencia un mercado en constante evolución dentro de la esfera cibercriminal. Las credenciales de usuarios robadas se convierten en una mercancía valiosa, subrayando la necesidad de una vigilancia y protección continua de la información digital.

Este caso sirve de recordatorio crítico sobre la persistente amenaza del ciberdelito y la importancia de adoptar medidas preventivas eficaces para salvaguardar la privacidad y seguridad en línea.

Fuente

Link de la Informacion