LITORALPRESS

Fecha: 25-06-2024
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: Hackers adquirieron $151 millones en productos de PC Factory sin pagar

Pág. : 7
Cm2: 340,3

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

El fraude ocurrió entre diciembre de 2023 y marzo de 2024

Hackers adquirieron $151 millones en productos de PC Factory sin pagar

IGNACIO MOLINA

PC Factory, una empresa especializada en la venta de productos tecnológicos, detectó una vulneración en sus sistemas de pago que permitió a clientes realizar compras sin pagar. Esta situación llevó a la compañía a presentar una querella en el 4° Juzgado de Garantía de Santiago contra todos quienes resulten responsables, en calidad de autores, cómplices o encubridores, por los delitos informáticos y estafa.

El total de las operaciones defectuosas asciende a 96. El perjuicio económico total fue de $151.384.760. Este fraude informático ocurrió entre diciembre de 2023 y el 31 de marzo de 2024.

Empresa dice que se aprovecharon de una vulnerabilidad del sistema de pago online.

Los productos fueron despachados o retirados por los compradores, quienes obtuvieron las boletas, aunque no se les realizó el cobro, según acusó la empresa.

La vulnerabilidad se habría producido por un error que permitía a los compradores omitir la etapa de pago mediante la modificación de herramientas del navegador.

Jonathan Frez, ingeniero civil en informática, con doctorado en Computación, explica cómo pudo haber sucedido este problema. Dice que cuando se visita una página web, como comprar en PC Factory, el servidor envía una copia de la página al navegador de nuestro computador, como si fuera una imagen de lo que vamos a ver. El navegador nos muestra esa imagen y nos permite hacer clic en elementos, como comprar productos.

"Es importante entender que esta es solo una versión para ser mostrada en tu computador, nada más", acota Frez, actual director del Posgrado de la Facultad de Ingeniería y Ciencias de la Universidad Diego Portales. "El navegador tiene una opción de desarrollador que habilita la edición de la copia que te está mostrando, similar a editar un documento. No edita la página en el servidor, solo la copia que te envió para ser mostrada", explica Silva.

El asunto de seguridad -añade- es que a veces la información de si pagamos o no también se envía junto con esa imagen.

RICHARD ULLOA

PC Factory sufrió pérdidas económicas totales por un monto de $151.384.760.

Esto permite que algunas personas usen herramientas especiales para cambiar esa información antes de que realmente paguen. Es como si alguien pudiera cambiar una boleta en papel de "pendiente de pago" a "pagado" antes de que el dinero realmente salga de la cuenta.

¿Cuáles serían las mejores prácticas para prevenir y detectar este tipo de vulnerabilidades?Según Nicolás Silva, ingeniero en computación y máster en Tecnología de la Información, es crucial realizar revisiones de hackeo ético en sitios que procesan muchas transacciones. "Esto implica contratar a una empresa o profesional para intentar vulnerar el sitio mediante diversos tipos de ataques", dice Silva, director de Tecnología de Asimov Consultores.

Esta medida preventiva -añade- permite identificar y corregir posibles vulnerabilidades antes de que sean explotadas. "Esto es especialmente importante en sitios que manejan pagos y dinero ya que siempre van a ser el foco de los ataques de delincuentes", advierte el ingeniero en computación.