

 Centro Nacional de Seguridad Digital		ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°304		Fecha: 22-12-2023
				Página: 4 de 7
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL			
Nombre de la alerta	Sitio falso de Mercado Libre dirigido a México busca robar información financiera			
Tipo de Ataque	Portal fraudulento	Abreviatura	PortalFrau	
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros			
Código de familia	G	Código de Sub familia	G02	
Clasificación temática familia	Fraude			
Descripción				
<p>1. ANTECEDENTES:</p> <p>A través de anuncios en Facebook se distribuye este sitio falso que suplanta la identidad de Mercado Libre y ofrece supuestos descuentos del 80%, sin embargo, su único propósito es robar los datos financieros de la víctima.</p> <p>2. DETALLES:</p> <p>En esta táctica conocida como phishing, los ciberdelincuentes crean un sitio con apariencia similar al oficial, esperando atrapar a víctimas distraídas que no verifiquen correctamente la URL. En este caso, el sitio falso se asemeja a la plataforma de compraventa, y ofrece supuestos descuentos de hasta 80 por ciento en gran cantidad de productos, con el fin de tentar a los usuarios a hacer clic en la publicidad, y engañarlos para que realicen un falso proceso de compra que solo llevará al robo de sus datos financieros.</p> <p>Al analizar el sitio reportado, se puede determinar que el usuario era redirigido a un sitio que simula ser MercadoLibre de manera convincente, aunque con detalles como logos antiguos y tipografía inconsistente. A pesar de estas imperfecciones, resulta atractivo para aquellos cautivados por ofertas tentadoras.</p> <p>La primera señal de alerta que se puede identificar fue que la URL es evidentemente falsa, y no tiene ninguna relación con el sitio oficial de la plataforma.</p> <p>La plataforma falsa permite ingresar datos de contacto de cualquier parte del mundo, pero solo ofrece la opción de seleccionar México como país, indicando una campaña dirigida específicamente a usuarios mexicanos. Además, las imágenes de portada hacen referencia a México, los precios figuran en la moneda local y métodos de pago adicionales que también son locales.</p> <p>El sitio presenta una interfaz ligeramente diferente a la real, permitiendo ingresar información de entrega del producto y datos financieros con aparente legitimidad. Durante la investigación, se descubrió que el sistema rechaza datos falsos al intentar ingresar números de tarjetas de crédito ficticias. Esta característica, sumada al buen diseño de la plataforma falsa y sus detalles cuidados, hace complicado percibir el engaño.</p> <p>los cibercriminales obtienen una base de datos financiera depurada y válida, lista para ser utilizada en compras fraudulentas o vendida en la dark web y otras plataformas utilizadas por ciberdelincuentes.</p> <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> • Evitar hacer clic en anuncios que te llamen la atención hasta que verifiques su autenticidad. • Desconfiar de ofertas y descuentos demasiado buenos para ser verdad. • Escribir la URL oficial del sitio que se desea visitar. • Denunciar cualquier intento de suplantación o phishing en la plataforma o sitio donde aparezcan estas falsas publicidades. 				
Fuente de Información:	<ul style="list-style-type: none"> • https://www.welivesecurity.com/es/estafas-enganos/sitio-falso-mercado-libre-mexico-robar-informacion-financiera/ 			