Los expertos en ciberseguridad han alertado sobre una nueva campaña de skimming de tarjetas de crédito que opera de manera discreta, enfocándose en las páginas de pago de sitios de comercio electrónico en WordPress. Esta técnica consiste en insertar código JavaScript malicioso dentro de una tabla de base de datos vinculada al sistema de gestión de contenido (CMS).

> *«Este malware, diseñado para robar datos de tarjetas de crédito en sitios de WordPress, añade JavaScript malicioso de manera silenciosa a entradas de bases de datos con el objetivo de capturar información confidencial de pago»,* explicó Puja Srivastava, investigadora de Sucuri, en un análisis reciente.
>
> *«El software malicioso se activa específicamente en las páginas de pago, tomando el control de los campos de pago legítimos o incorporando un formulario falso para tarjetas de crédito»,* añadió.

La compañía de seguridad web, propiedad de GoDaddy, identificó que el malware estaba oculto en la tabla `wp_options` de WordPress bajo la opción «widget_block». Esto le permite evadir herramientas de detección y mantenerse en los sitios infectados sin levantar sospechas.

El mecanismo de ataque utiliza el panel de administración de WordPress (`wp-admin > widgets`) para incrustar el JavaScript malicioso en un bloque HTML.

Este código malicioso detecta si la página actual es de checkout y se activa únicamente cuando el usuario está a punto de ingresar sus datos de pago. En ese momento, genera de forma dinámica una pantalla de pago fraudulenta que imita a procesadores de pago reconocidos como Stripe.

El formulario falso recopila información como el número de la tarjeta de crédito, fecha de vencimiento, código CVV e información de facturación. Además, el script también puede

interceptar los datos ingresados en formularios legítimos en tiempo real, asegurando así su funcionalidad en diversos entornos.

Los datos capturados se codifican en Base64 y se cifran utilizando AES-CBC, lo que los hace parecer inofensivos y dificulta su análisis. Finalmente, esta información es enviada a un servidor controlado por los atacantes, como «valhafather[.]xyz» o «fqbe23[.]xyz».

Este incidente ocurre poco después de que Sucuri revelara otra campaña similar, en la que se utilizó malware JavaScript para generar formularios falsos de tarjetas de crédito o extraer datos ingresados en campos de pago.

La información recolectada pasa por tres niveles de ofuscación: se codifica como JSON, se cifra mediante XOR utilizando la clave «script» y, finalmente, se codifica en Base64 antes de ser enviada a un servidor remoto, como «staticfonts[.]com».

> *«El malware está diseñado para extraer información sensible de los campos de pago en las páginas de checkout. Además, recopila datos adicionales del usuario a través de las API de Magento, incluyendo nombre, dirección, correo electrónico, número de teléfono y detalles de facturación, utilizando los modelos `customer-data` y `quote` de Magento»,* explicó Srivastava.

En paralelo, se ha identificado una campaña de phishing con fines económicos que engaña a los usuarios mediante correos electrónicos que los dirigen a páginas de inicio de sesión de PayPal, simulando una solicitud de pago pendiente de aproximadamente $2,200.

> *«Los atacantes registraron un dominio de prueba de Microsoft 365, gratuito durante tres meses, y crearon una lista de distribución (`Billingdepartments1[@]gkjyryfjy876.onmicrosoft.com`) con correos electrónicos de las víctimas. Luego, solicitaron el dinero en el portal web de PayPal, añadiendo la lista de distribución como destinatario»*, detalló Carl Windsor, de

> Fortinet FortiGuard Labs.

Lo que hace que esta táctica sea especialmente engañosa es que los correos provienen de una dirección legítima de PayPal (`service@paypal.com`) e incluyen un enlace de inicio de sesión auténtico, lo que les permite evadir las herramientas de seguridad.

Para agravar la situación, cuando la víctima intenta iniciar sesión en su cuenta de PayPal, su perfil se vincula automáticamente a la dirección de correo electrónico de la lista de distribución, otorgando a los atacantes el control de la cuenta.

Además, en las últimas semanas se ha detectado que actores maliciosos están utilizando una técnica novedosa conocida como *«suplantación de simulación de transacciones»* para robar criptomonedas de las billeteras digitales de las víctimas.

> *«Las billeteras modernas de Web3 incluyen la simulación de transacciones como una herramienta amigable para el usuario. Esta función permite a los usuarios visualizar el resultado previsto de sus transacciones antes de firmarlas. Aunque está diseñada para mejorar la transparencia y la experiencia del usuario, los ciberdelincuentes han encontrado maneras de abusar de este sistema»*, explicó Scam Sniffer.

Los esquemas de infección se basan en aprovechar el lapso de tiempo entre la simulación y la ejecución de una transacción, permitiendo a los atacantes crear sitios fraudulentos que imitan aplicaciones descentralizadas (DApps) con el objetivo de robar fondos de las billeteras.

> *«Este tipo de ataque introduce un avance preocupante en las técnicas de phishing. En lugar de recurrir únicamente al engaño tradicional, los atacantes están manipulando funciones confiables de las billeteras que los usuarios consideran seguras. Este método más avanzado hace que su detección sea especialmente*

> *difícil»*, afirmó la empresa especializada en prevención de estafas Web3.