Diversas plataformas de gestión de contenido (CMS) como WordPress, Magento y OpenCart han sido blanco de un nuevo skimmer de tarjetas de crédito denominado Caesar Cipher Skimmer.

Un skimmer web es un tipo de malware que se introduce en sitios de comercio electrónico con el propósito de robar información financiera y de pago.

Según Sucuri, la campaña más reciente implica realizar modificaciones maliciosas en el archivo PHP de pago asociado al plugin WooCommerce para WordPress («form-checkout.php») con el fin de robar los datos de las tarjetas de crédito.

> *«En los últimos meses, las inyecciones se han modificado para parecer menos sospechosas que un script largo y ofuscado,»* explicó el investigador de seguridad Ben Martin, señalando el intento del malware de hacerse pasar por Google Analytics y Google Tag Manager.

Específicamente, utiliza el mismo mecanismo de sustitución empleado en el cifrado César para codificar la pieza de código malicioso en una cadena incomprensible y ocultar el dominio externo utilizado para alojar la carga maliciosa.

Se cree que todos los sitios web ya habían sido comprometidos previamente mediante otros métodos para implementar un script PHP conocido como «style.css» y «css.php» en un aparente esfuerzo por imitar una hoja de estilo HTML y evitar la detección.

Estos scripts, a su vez, están diseñados para cargar otro código JavaScript ofuscado que crea un WebSocket y se conecta a otro servidor para obtener el skimmer real.

> *«El script envía la URL de las páginas web actuales, lo que permite a los atacantes enviar respuestas personalizadas para cada sitio infectado. Algunas versiones del script de segunda capa incluso verifican si está siendo cargado por un usuario de*

> *WordPress con sesión iniciada y modifican la respuesta para ellos»,* indicó Martin.

Algunas versiones del script tienen comentarios escritos en ruso, lo que sugiere que los autores de esta operación son hablantes de ruso.

El archivo form-checkout.php en WooCommerce no es el único método utilizado para desplegar el skimmer, ya que también se ha observado a los atacantes utilizando de manera indebida el plugin legítimo WPCode para inyectarlo en la base de datos del sitio web.

En los sitios que usan Magento, las inyecciones de JavaScript se realizan en tablas de bases de datos como core_config_data. Actualmente, no se sabe cómo se logra esto en los sitios de OpenCart.

Debido a su uso generalizado como base para sitios web, WordPress y el amplio ecosistema de plugins se han convertido en un objetivo atractivo para los actores maliciosos, permitiéndoles acceder fácilmente a una gran superficie de ataque.

Es crucial que los propietarios de sitios mantengan su software CMS y plugins actualizados, practiquen una buena higiene de contraseñas y auditen periódicamente sus sitios en busca de cuentas de administrador sospechosas.