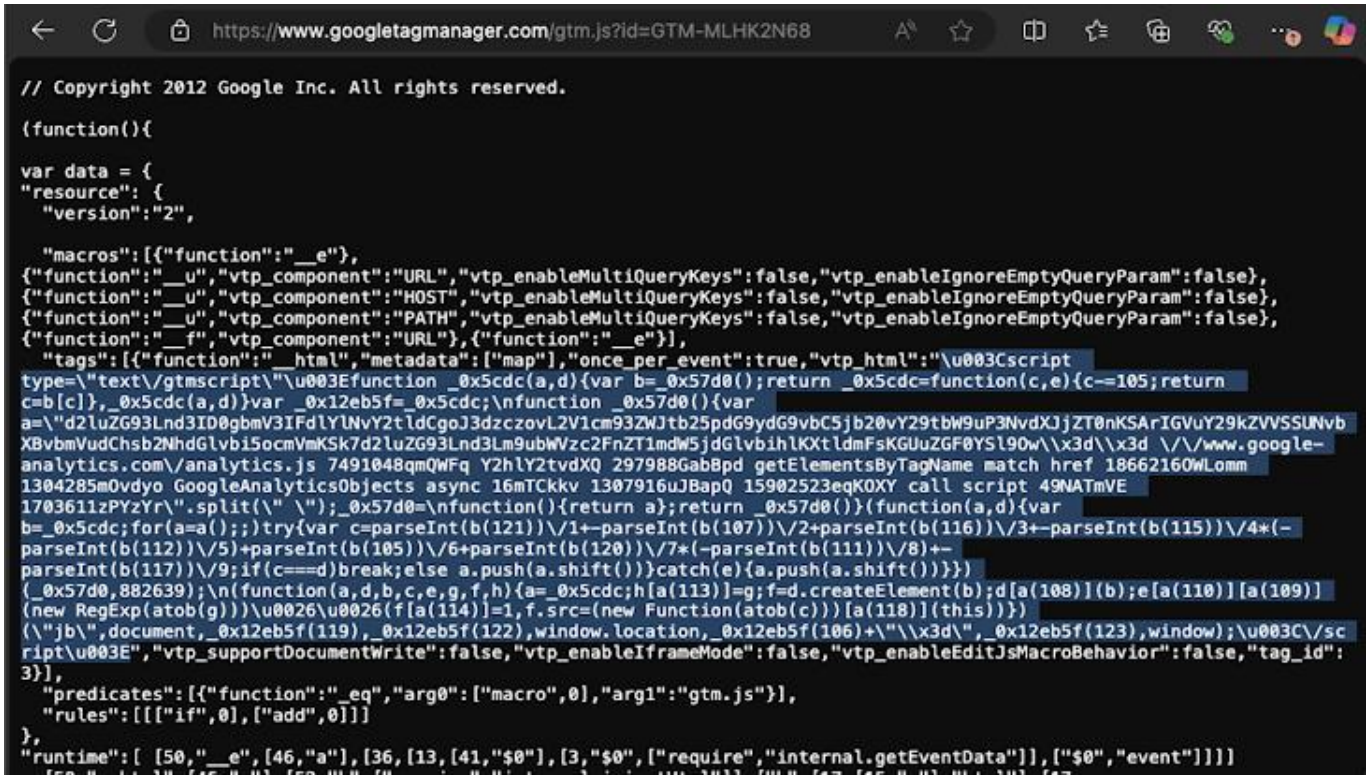
Los ciberdelincuentes han sido detectados utilizando Google Tag Manager (GTM) para distribuir un malware de skimming de tarjetas de crédito en sitios de comercio electrónico que operan con Magento.

La empresa de seguridad web Sucuri informó que el código malicioso, aunque aparenta ser un script legítimo de GTM y Google Analytics utilizado para análisis y publicidad en sitios web, en realidad oculta una puerta trasera diseñada para otorgar acceso continuo a los atacantes.

Hasta el momento, se han identificado al menos tres sitios afectados con el identificador de GTM (GTM-MLHK2N68), lo que representa una disminución respecto a los seis que Sucuri detectó inicialmente. Un identificador de GTM hace referencia a un contenedor que agrupa diversos códigos de seguimiento (como Google Analytics o Facebook Pixel) junto con reglas que se activan bajo ciertas condiciones.

Un análisis más profundo determinó que el malware proviene de la tabla «cms_block.content» en la base de datos de Magento, donde la etiqueta GTM carga un código JavaScript codificado que actúa como un skimmer de tarjetas de crédito.

> *«Este script fue diseñado para capturar información confidencial ingresada por los usuarios durante el proceso de pago y enviarla a un servidor remoto controlado por los atacantes»,* señaló la investigadora de seguridad Puja Srivastava.



Al ejecutarse, el malware extrae los datos de las tarjetas de crédito desde las páginas de pago y los transfiere a un servidor externo.

No es la primera ocasión en la que GTM se ha explotado con fines maliciosos. En abril de 2018, Sucuri reveló que esta herramienta había sido utilizada en campañas de publicidad fraudulenta (malvertising).

Este nuevo ataque ocurre pocas semanas después de que la empresa expusiera otra campaña que afectó sitios web en WordPress. En ese caso, los atacantes probablemente explotaron vulnerabilidades en plugins o accedieron a cuentas de administrador comprometidas para instalar un malware que redirigía a los visitantes a páginas web maliciosas.