Investigadores de seguridad cibernética descubrieron una nueva campaña de skimmer web en curso al estilo de Magecart, que está diseñada para robar información de identificación personal (PII) y datos de tarjetas de crédito de sitios web de comercio electrónico.

Un aspecto digno de mención que lo diferencia de otras campañas de Magecart es que los sitios secuestrados sirven también como servidores de comando y control (C2) *«improvisados»,* usando la cubierta para facilitar la distribución de código malicioso sin el conocimiento de los sitios de las víctimas.

La empresa de seguridad web Akamai, dijo que identificó víctimas de diversos tamaños en América del Norte, América Latina y Europa, lo que podría poner los datos personales de miles de visitantes del sitio web en riesgo de ser recolectados y vendidos para obtener ganancias ilícitas.

> *«Los atacantes emplean una serie de técnicas de evasión durante la campaña, incluyendo la ofuscación en Base64 y el enmascarado del ataque para parecerse a servicios populares de terceros, como Google Analytics o Google Tag Manager»,* dijo Roman Lvovsky, investigador de seguridad de Akamai.

La idea, de forma general, es violar sitios legítimos vulnerables y usarlos para alojar código de skimmer web, aprovechando así la buena reputación de los dominios genuinos en su beneficio. En algunos casos, los ataques han estado en marcha por casi un mes.

> *«En lugar de usar el propio servidor C2 de los atacantes para alojar código malicioso, que puede marcarse como un dominio malicioso, los atacantes hackean (usando vulnerabilidades o cualquier otro medio a su disposición) un sitio legítimo y vulnerable, como un sitio pequeño o mediano, minorista de tamaño reducido y guardan su código en él»,* dijo Akamai.

El resultado de los ataques son dos tipos de víctimas: sitios legítimos que se han visto comprometidos para actuar como un *«centro de distribución»* de malware y sitios web de comercio electrónico vulnerables que son el objetivo de los skimmers.

En algunos casos, los sitios web no solo han sido objeto de robo de datos, sino que también han servido sin saberlo como un vehículo para propagar el malware a otros sitios web susceptibles.

> *«Este ataque incluyó la explotación de Magento, WooCommerce, WordPress y Shopify, lo que demuestra la creciente variedad de vulnerabilidades y plataformas de comercio digital abusables»,* dijo Lvovsky.

Al aprovechar la confianza establecida que los sitios web han ganado con el tiempo, la técnica crea una *«cortina de humo»* que dificulta identificar y responder a dichos ataques.

La campaña también adopta otros métodos para evitar la detección. Esto incluye camuflar el código del skimmer como servicios de terceros como Google Tag Manager o Facebook Pixel para ocultar sus verdaderas intenciones.

Otro truco empleado es que los fragmentos del código JavaScript funcionan como cargadores para obtener el código de ataque completo del sitio web de la víctima host, lo que minimiza la huella y la probabilidad de detección.

El código de skimmer ofuscado, que viene en dos variantes distintas, está equipado para interceptar y exfiltrar PII y detalles de tarjetas de crédito como una cadena codificada por medio de una solicitud HTTP a un servidor controlado por un atacante.

> *«La exfiltración solo ocurrirá una vez por cada usuario que pase por la caja. Una vez que se roba la información de un usuario, el script marcará el navegador para asegurarse de que no robe la información dos veces (para reducir el tráfico de red sospechoso). Esto aumenta aún más la capacidad de evasión de este ataque al estilo Magecart»,* dijo Lvovsky.