Investigadores de seguridad cibernética informaron este lunes que un grupo de hackers está explotando el servicio de Google Analytics para robar información de tarjetas de crédito de sitios de comercio electrónico infectados.

Según los informes independientes de PerimeterX, Kaspersky y Sansec, los actores de amenazas están inyectando código de robo de datos en los sitios web comprometidos en combinación con el código de seguimiento generado por Google Analytics para su propia cuenta, lo que les permite filtrar la información de pago ingresada por los usuarios en condiciones donde las políticas de seguridad de contenido se aplican para la máxima seguridad web.

> *«Los atacantes inyectaron código malicioso en los sitios, que recopilaron todos los datos ingresados por los usuarios y luego los enviaron a través de Analytics. Como resultado, los atacantes pueden acceder a los datos robados de Google Analytics»*, dijo Kaspersky.

La compañía de seguridad también dijo que encontró cerca de dos docenas de sitios web infectados en Europa y América del Norte y del Sur, que se especializaron en la venta de equipos digitales, cosméticos, productos alimenticios y repuestos.

El ataque depende de la premisa de que los sitios web de comercio electrónico que usan el servicio de análisis web de Google para rastrear visitantes, han incluido en la lista blanca los dominios asociados en su política de seguridad de contenido (CSP).

CSP es una medida adicional de seguridad que ayuda a detectar y mitigar las amenazas derivadas de las vulnerabilidades de secuencias de comandos en sitios cruzados y otras formas de ataques de inyección de código, incluidos los adoptados por varios grupos de Magecart.

Esta función de seguridad permite a los webmasters definir un conjunto de dominios con los que se debe permitir que el navegador web interactúe para una URL específica, evitando así la ejecución de código no confiable.

> *«La fuente del problema es que el sistema de reglas CSP no es lo suficientemente granular. Reconocer y detener la solicitud JavaScript maliciosa anterior requiere soluciones de visibilidad avanzadas que pueden detectar el acceso y la filtración de datos confidenciales del usuario (en este caso, la dirección de correo electrónico y contraseña del usuario)»*, dijo Amir Shaked, vicepresidente de investigación de PerimeterX.

Para recopilar datos utilizando esta técnica, todo lo que se necesita es un fragmento de código JavaScript que transmita los detalles recopilados, como las credenciales y la información de pago, por medio de un evento y otros parámetros que Google Analytics utiliza para identificar de forma única las diferentes acciones realizadas en un sitio.

> *«Los administradores escriben *.google-analytics.com en el encabezado Content-Security-Policy (utilizado para enumerar los recursos de los que se puede descargar el código de terceros), permitiendo que el servicio recopile datos. Además, el ataque se puede implementar sin descargar el código de fuentes externas»,* informó Kaspersky.

Para hacer que los atacantes sean más encubiertos, los atacantes también determinan si el modo desarrollador, una característica que por lo general se utiliza para detectar solicitudes de red y errores de seguridad, está habilitado en el navegador del visitante y procede solo si el resultado de esa verificación es negativo.

Por otro lado, Sansec describió en su informe que descubrió una campaña similar desde el 17 de marzo, que entregó el código malicioso en varias tiendas utilizando un código JavaScript

alojado en Firebase de Google.

Para la ofuscación, el actor detrás de la operación creó un iFrame temporal para cargar una cuenta de Google Analytics controlada por el atacante. Los datos de la tarjeta de crédito ingresados en los formularios de pago se cifran y se envían a la consola de análisis desde donde se recuperan utilizando la clave de cifrado usada anteriormente.

Debido al uso generalizado de Google Analytics en estos ataques, las contramedidas como CSP no funcionarán si los atacantes aprovechan un dominio ya permitido para secuestrar información confidencial.

> *«Una posible solución vendría de las URL adaptables, agregando la ID como parte de la URL o subdominio para permitir a los administradores establecer reglas CSP que restrinjan la exfiltración de datos a otras cuentas»,* dijo Shaked.
>
> *«Una dirección futura más granular para fortalecer la dirección de CSP a considerar como parte del estándar CSP es la aplicación de proxy XHR. Esto esencialmente creará un WAF del lado del cliente que puede aplicar una política sobre dónde se pueden transmitir los campos de datos específicos»*, agregó.