En una campaña de piratería innovadora, los hackers están ocultando implantes de códigos maliciosos en los metadatos de archivos de imagen para robar en secreto información de tarjetas bancarias de los visitantes.

> *«Encontramos código de ocultación dentro de los metadatos de un archivo de imagen (una forma de esteganografía), y cargado subrepticiamente por tiendas en línea comprometidas»,* dijeron los investigadores de Malwarebytes.
>
> *«Este esquema no estaría completo sin otra variación interesante para extraer datos de tarjetas de crédito robadas. Una vez más, los delincuentes usaron el disfraz de un archivo de imagen para recolectar su botín».*

La táctica evolutiva de la operación, ampliamente conocida como descremado web o ataque Magecart, se produce cuando los atacantes encuentran diferentes formas de inyectar código JavaScript, incluidos los cubos de almacenamiento de datos AWS S3 mal configurados y explotar la política de seguridad de contenido para transmitir datos a una cuenta de Google Analytics bajo su control.

El uso de técnicas de esteganografía generalmente funcionan al insertar código malicioso en un sitio web comprometido, que recolecta y envía subrepticiamente datos ingresados por el usuario al servidor de un pirata informático, lo que le brinda acceso a la información de pago de los compradores.

En esta campaña de una semana, la compañía de seguridad cibernética descubrió que el skimmer no solo se descubrió en una tienda en línea que ejecuta el complemento WooCommerce WordPress, sino que estaba contenido en los metadatos EXIF (formato de archivo de imagen intercambiable) de un favicon para un dominio sospechoso (cddn.site).

Cada imagen se incrusta con información sobre la imagen en sí, como el fabricante y modelo de la cámara, fecha y hora en que se tomó la foto, ubicación, resolución y la configuración de la cámara, entre otros detalles.

Utilizando estos datos EXIF, los hackers ejecutaron un fragmento de JavaScript que estaba oculto en el campo «Copyright» de la imagen favicon.

> *«Al igual que con otros skimmers, este también capta el contenido de los campos de entrada donde los compradores en línea ingresan su nombre, dirección de facturación y detalles de tarjeta de crédito»,* dijeron los investigadores.

Además de codificar la información capturada utilizando el formato Base64 e invertir la cadena de salida, los datos robados se transmiten en forma de un archivo de imagen para ocultar el proceso de exfiltración.

Al afirmar que la operación podría ser obra de Group 9 de Magecart, Malwarebytes dijo que el código JavaScript para el skimmer se ofusca con la biblioteca WiseLoop PHP JS Obfuscator.

Esta no es la primera vez que los grupos de Magecart utilizan imágenes como vectores de ataque para comprometer los sitios web de comercio electrónico. En mayo, se observó que distintos sitios web pirateados cargaban un favicon malicioso en sus páginas web de pago y luego reemplazaban los formularios de pago en línea legítimos con un sustituto fraudulento que robada los datos de la tarjeta.

Abuso del protocolo DNS para filtrar datos del navegador

En una técnica separada demostrada por Jessie Li, demuestra que es posible robar datos del navegador aprovechando dns-prefetch, un método de reducción de latencia utilizado para resolver búsquedas de DNS en dominios de origen cruzado antes de solicitar recursos.

Llamado «browsertunnel«, el software de código abierto consiste en un servidor que decodifica los mensajes enviados por la herramienta y una biblioteca JavaScript del lado del cliente para codificar y transmitir los mensajes.

En sí, los mensajes son cadenas arbitrarias codificadas en un subdominio del dominio superior que el navegador está resolviendo. Después, la herramienta escucha las consultas DNS, recopila los mensajes entrantes y los decodifica para extraer los datos relevantes.

En otras palabras, browsertunnel se puede utilizar para acumular información confidencial a medida que los usuarios realizan acciones específicas en una página web y posteriormente las filtra a un servidor disfrazándola como tráfico DNS.

> *«El tráfico DNS no aparece en las herramientas de depuración del navegador, no está bloqueado por la Política de Seguridad de Contenido (CSP) de una página, y a menudo no es inspeccionado por firewalls o proxies corporativos, lo que lo convierte en un medio ideal para el contrabando de datos en escenarios restringidos»,* dijo el investigador.