Investigadores de seguridad cibernética descubrieron que más de 80 sitios web de comercio electrónico comprometidos de Magecart, enviaban activamente información de tarjetas de crédito de compradores en línea a los servidores controlados por los atacantes.

Muchos de estos sitios web son de marcas de renombre en Estados Unidos, Canadá, Europa, América Latina y Asia, según revelaron los investigadores de Aite Group y Arxan Technologies.

Magecart es un término general que se le dio a diferentes grupos de delincuentes cibernéticos que se especializan en implantar de forma secreta skimmers de tarjetas de crédito en línea en sitios web de comercio electrónico comprometidos, con la intención de robar los detalles de las tarjetas de sus clientes.

Estos skimmers virtuales, también conocidos como ataques de formjacking, son básicamente un código JavaScript que los hackers insertan en secreto en un sitio web comprometido, generalmente en la página del carrito de compras, diseñado para capturar información de pago de los clientes en tiempo real y enviarlo a un atacante remoto.

Magecart ha sonado mucho en los medios últimamente por llevar a cabo robos de alto perfil contra compañías importantes como British Airways, Ticketmaster, Newegg, entre otras.

La campaña recientemente divulgada no pertenece a un solo grupo de hackers de Magecart, los investigadores utilizaron un motor de búsqueda de código fuente para encontrar JavaScript ofuscado en Internet con patrones maliciosos que se vieron previamente en los skimmers de tarjetas virtuales de Magecart.

Según los investigadores, la técnica les permitió descubrir rápidamente más de 80 sitios web de comercio electrónico comprometidos por grupos de Magecart, la mayoría de los cuales se encuentran ejecutando versiones desactualizadas de Magento CMS que son vulnerables a una carga no autenticada y vulnerabilidades de ejecución remota de código.

> *«La ausencia de protección en la aplicación, como la ofuscación del código y la detección de manipulación, hace que las aplicaciones web sean vulnerables a un tipo de ciberataque llamado formjacking»*, detallaron los investigadores.
>
> *«Muchos de los sitios comprometidos ejecutan la versión 1.5, 1.7 o 1.9. La carga arbitraria de archivos, la ejecución remota de código y las vulnerabilidades de falsificación de solicitudes entre sitios afectan a Magento versión 2.1.6 y posteriores. Si bien no se puede declarar con autoridad que esto es lo que llevó a la violación de estos sitios, estas son versiones vulnerables de Magento que permiten a los adversarios inyectar el código de formulario en el sitio».*

Aunque los investigadores no nombraron a las compañías comprometidas en su informe, trabajaron con las fuerzas del orden federales para notificar a todas las organizaciones afectadas, así como a los servidores externos antes de publicar su informe.

> *«Debido a que este es un proyecto en curso y activo, hemos decidido no nombrar los sitios de las víctimas»*, dijeron los investigadores.

Además, los investigadores también analizaron las actividades de monetización de Magecart y descubrieron que, además de vender los datos de la tarjeta de pago robada en los foros web oscuros, los atacantes también compran mercancías en sitios legítimos de compras en línea y las envían a mulas de mercancías preseleccionadas en un intento de lavado.

> *«Para reclutar mulas de mercancías, el atacante publica trabajos que ofrecen a las personas la capacidad de trabajar desde casa y ganar grandes sumas de dinero para recibir y reenviar mercancías compradas con los números de tarjetas de crédito robadas»,* agregaron los investigadores.

Después, las mulas trabajan con los cargadores locales que reciben un pago por debajo de la mesa para el envío de la mercancía a los destinos de Europa del este, donde se vende a compradores locales, lo que finalmente beneficia a los atacantes como una segunda línea de ingresos.

Los investigadores recomiendan a los administradores de sitios web de comercio electrónico, actualizar el software de su plataforma a la última versión que los proteja de exploits conocidos.

Además, los sitios web de comercio electrónico también deben implementar la ofuscación de código y la criptografía de caja blanca para hacer que los formularios web sean ilegibles para el adversario, así como soluciones para detectar modificaciones no autorizadas de los archivos del sitio web.

También se recomienda a los compradores en línea que revisen continuamente los detalles de su tarjeta y los estados de cuenta bancarios, para detectar cualquier actividad desconocida.