Los hackers siguen aprovechando los cubos de almacenamiento de datos AWS S3 mal configurados para insertar código malicioso en sitios web con el fin de obtener la información de tarjetas de crédito y realizar campañas de publicidad maliciosas.

En un nuevo informe, la compañía de seguridad cibernética, RiskIQ, dijo que identificó el mes pasado tres sitios web comprometidos que pertenecen a Endeavor Business Media y que aún alojan código para skimming en JavaScript, una táctica adoptada por Magecart, una organización de distintos grupos de hackers que se dirigen en línea a sistemas con carrito de compras.

Los sitios web afectados sin parches alojan contenido relacionado con servicios de emergencia y foros de chat que atienden bomberos, policías y profesionales de seguridad, según RiskIQ.

Los sitios afectados son: www[.]officer[.]com, www[.]firehouse[.]com y www[.]securityinfowatch[.]com.

La compañía de seguridad dijo que no ha recibido noticias de Endeavor Business Media a pesar de haberse comunicado con la empresa para intentar abordar los problemas.

Ahora, RiskIQ está trabajando con la firma suiza de ciberseguridad sin fines de lucro, Abuse.ch, para hundir los dominios maliciosos asociados con la campaña.

Amazon S3 (Simple Storage Service), es una infraestructura de almacenamiento escalable que ofrece un medio confiable para guardar y recuperar cualquier cantidad de datos por medio de una interfaz de servicios web.

Estos skimmers virtuales de tarjetas de crédito, también conocidos como ataques de formjacking, son típicamente código JavaScript que los operadores de magecart insertan de forma sigilosa en un sitio web comprometido, por lo general, en páginas de pago, diseñado para capturar los detalles de las tarjetas de los clientes en tiempo real y transmitirlo a un servidor remoto.

En julio pasado, RiskIQ descubrió una campaña similar de Magecart que aprovechaba los cubos S3 mal configurados para inyectar skimmers de tarjetas de crédito digitales en 17 mil dominios.

Además de utilizar JavaScript para cargar el skimmer, RiskIQ dijo que descubrió un código adicional que llama *«jqueryapi1oad»*, usado en conexión con una operación de publicidad maliciosa de larga duración que comenzó en abril de 2019 y ha infectado 277 hosts únicos hasta la fecha.

> *«Primero identificamos el redireccionador malicioso jqueryapi1oad, llamado así por la cookie que conectamos en él, en julio de 2019. Nuestro equipo de investigación determinó que los actores detrás del código malicioso también estaban explotando cubos S3 mal configurados*«, dijeron los investigadores.

El código establece la cookie jqueryapi1oad con una fecha de vencimiento basada en el resultado de una verificación de bot y crea un nuevo elemento DOM en la página en la que se inyectó. Después, procede a descargar código JavaScript adicional que, a su vez, carga una cookie asociada con el sistema de distribución de tráfico Keitaro (TDS) para redirigir el tráfico a los anuncios fraudulentos vinculados a la campaña de publicidad maliciosa de HookAds.

> *«El dominio futbolred[.]com es un sitio de noticias de fútbol colombiano que se encuentra en el top 30,000 de las clasificaciones mundiales de Alexa. También configuró mal un cubo S3, dejándolo abierto a jqueryapi1oad»,* agregaron los investigadores.

Para mitigar estas amenazas, RiskIQ recomienda asegurar los depósitos de S3 con el nivel correcto de permisos, además de utilizar las Listas de Control de Acceso (ACL) y las políticas de depósito para otorgar acceso a otras cuentas de AWS o solicitudes públicas.

> *«Los paquetes S3 mal configurados que permiten a los actores maliciosos insertar su código en numerosos sitios web es un problema continuo. En el entorno de amenazas actual, las empresas no pueden avanzar de forma segura sin tener una huella digital, un inventario de todos los archivos digitales, para garantizar que estén bajo la administración de su equipo de seguridad configurados adecuadamente».*