Hackean más de 2000 tiendas Magento durante el fin de semana

Autor: I. Stepanenko

Fecha: Sunday 27th of September 2020 03:47:28 PM

Más de 2000 tiendas en línea de Magento fueron hackeadas durante el fin de semana en un acto que los investigadores de seguridad cibernética describieron como *«la campaña más grande de la historia»*.

Los ataques fueron un esquema típico de Magecart, donde los hackers violaron sitios y luego colocaron scripts maliciosos dentro del código fuente de las tiendas, código que registraba los detalles de las tarjetas de pago que los compradores ingresaban dentro de los formularios de pago.

> «El viernes, 10 tiendas se infectaron, luego 1058 el sábado, 603 el domingo y 233 hoy», dijo Willem de Groot, fundador de Sanguine Security (SanSec).

> «Esta campaña automatizada es, por mucho, la más grande que Sansec ha identificado desde que comenzó a monitorear en 2015. El récord anterior fue de 962 tiendas pirateadas en un solo día en julio del año pasado», agregó.

El ejecutivo de SanSec dijo también que la mayoría de los sitios comprometidos estaban ejecutando la versión 1.x del software de tienda en línea Magento.

Esta versión de Magento llegó al ginal de su vida útil (EOL) el 30 de junio de 2020, y actualmente ya no recibe actualizaciones de seguridad.

Cabe mencionar que los ataques contra sitios que ejecutan Magento 1.x se anticiparon desde el año pasado, cuando Adobe, propietario de Magento, emitió la primera alerta en noviembre de 2019 sobre la necesaria actualización a la rama 2.x.

La advertencia inicial de Adobe sobre ataques inminentes a las tiendas Magento 1.x se hizo eco más tarde en avisos de seguridad similares emitidos por Mastercard y Visa durante la primavera.

Aunque de Groot no ha identificado cómo los hackers irrumpieron en los sitios que fueron atacados durante el fin de semana, el fundador de SanSec dijo que el mes pasado se había publicado anuncios de una vulnerabilidad de día cero en Magento 1.x en foros de hacking clandestinos, lo que confirma que los piratas informáticos habían esperado que llegara la EOL.

En el anuncio, un usuario con el nombre *z3r0day*, ofreció en venta un exploit de ejecución remota de código (RCE) por 5 mil dólares, una oferta considerada increíble en ese momento.

Desde noviembre de 2019, cuando Adobe comenzó a advertir a los usuarios de Magento que migren a la versión más nueva, el número de tiendas Magento 1.x bajó de 240,000 a 110,000 en junio de 2020, y a 98,000 en la actualidad.