Una ola de ataques cibernéticos ocurrida contra los minoristas que ejecutan la plataforma de comercio electrónico Magento 1.x a inicios de septiembre ha atribuido a un solo grupo, según la última investigación.

> *«Este grupo ha llevado a cabo una gran cantidad de diversos ataques Magecart que por lo general comprometen una gran cantidad de sitios web a la vez a través de ataques a la cadena de suministro, como el incidente de Adverline, o mediante el uso de exploits como en los ataques a Magento del 1 de septiembre»*, dijo RiskIQ en un análisis.

Llamados colectivamente como Cardbleed, los ataques se dirigieron al menos a 2806 sitios web que ejecutaban Magento 1.x, versión que llegó al final de su vida útil el 30 de junio de 2020.

Inyectar e-skimers en sitios web de compras para robar datos de tarjetas de crédito es una actividad probada y comprobada de Magecart, un consorcio de distintos grupos de hackers que apuntan a los sistemas de carritos de compras en línea.

Estos skimmers de tarjetas virtuales, también conocidos como ataques de formjacking, suelen ser de código JavaScript que los operadores insertan de forma sigilosa en un sitio web de comercio electrónico, a menudo en páginas de pago, con la intención de capturar los detalles de la tarjeta de los clientes en tiempo real y transmitirlos a un servidor remoto controlado por un atacante.

Pero en los últimos meses, los operadores de Magecart intensificaron sus esfuerzos para ocultar el código del ladrón de tarjetas dentro de los metadatos de la imagen e incluso llevar a cabo ataques homógrafos de IDN para plantar skimmers web ocultos en el archivo favicon del sitio web.

Cardbleed, que fue documentado por primera vez por Sansec, funciona mediante el uso de dominios específicos para interactuar con el panel de administración de Magento, y luego,

aprovecha la función *«Magento Connect»* para descargar e instalar un malware llamado *«mysql.php»* que se elimina de forma automática luego de que el código del skimmer se agrega a *«prototype.js»*.

Ahora, según la investigación de RiskIQ, los ataques tienen todos los sellos distintivos de un solo grupo al que rastrea como Magecart Group 12 según las superposiciones en la infraestructura y las técnicas en distintos ataques, comenzando con Adverline en enero de 2019 hasta los revendedores de boletos de los Juegos Olímpicos en febrero de 2020.

Además, el skimmer utilizado en los compromisos es una variante del skimmer de hormigas y cucarachas observado por primera vez en agosto de 2019, llamado así por una función etiquetada «ant_cockcroach ()» y una variable «ant_check» que se encuentra en el código.

Uno de los dominios (myicons[.]net) observados por los investigadores, también vincula al grupo a otra campaña llevada a cabo en mayo, donde se utilizó el archivo de favicon de Magento para ocultar el skimmer en las páginas de pago y cargar un formulario de pago falso para robar información capturada.

Pero justo cuando se están eliminando los dominios maliciosos identificados, Group 12 se ha convertido en experto en intercambiar nuevo dominios para seguir con el rastreo.

> *«Desde que se publicitó la campaña, los atacantes han barajado su infraestructura. Se movieron para cargar el skimmer de ajaxcloudflare[.]com, que también ha estado activo desde mayo y trasladaron la exfiltración a un dominio registrado recientemente, consoler[.]in»,* dijeron los investigadores de RiskIQ.

En todo caso, los ataques son otro indicio de que los actores de amenazas siguen innovando, jugando con diferentes formas de hacer skimming y ofuscando su código para evadir la detección, dijo el investigador de RiskIQ, Jordan Herman.

> *«El motivo de esta investigación fue el compromiso generalizado de Magento 1, que dejó de funcionar este junio. Entonces, la mitigación particular sería actualizar a Magento 2, aunque el costo de la actualización podría ser prohibitivo para los proveedores más pequeños»*, dijo Herman.
>
> *«También hay una empresa llamada Mage One, que sigue apoyando y parcheando Magento 1. A fines de octubre lanzaron un parche para mitigar la vulnerabilidad particular explotada por el actor. En última instancia, la mejor forma de prevenir este tipo de ataques es por tiendas electrónicas de comercio que tienen un inventario completo del código que se ejecuta en su sitio para que puedan identificar las versiones obsoletas del software y cualquier otra vulnerabilidad que pueda invitar a un ataque Magecart»*, agregó.