Los grupos de hackers de Magecart están utilizando el servicio de mensajería instantánea Telegram para enviar detalles de pago robados de sitios web comprometidos, como una nueva forma de beneficio de los servicios cifrados de extremo a extremo y API que ofrece la aplicación.

> *«Para los actores de amenazas, este mecanismo de exfiltración de datos es eficiente y no requiere que mantengan una infraestructura que podría ser derribada o bloqueada por los defensores. Incluso, pueden recibir una notificación en tiempo real para cada nueva víctima, ayudándoles a monetizar rápidamente las tarjetas robadas en los mercados clandestinos», dijo Jérome Segura,* de Malwarebytes.

El TTP fue documentado públicamente por primera vez por el investigador de seguridad @AffableKraut en Twitter la semana pasada, utilizando datos de la compañía holandesa de seguridad, Sansec.

Imagen: Malwarebytes

La forma conocida en que operan los grupos de Magecart es inyectar e-skimmers en los sitios web de compras mediante la explotación de una vulnerabilidad conocida o credenciales robadas para obtener los detalles de tarjetas bancarias.

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

En los últimos meses, se han intensificado los esfuerzos por ocultar el código del ladrón de tarjetas dentro de los metadatos de las imágenes, e incluso llevar a cabo ataques homógrafos de IDN para plantar skimmers ocultos en el archivo favicon de un sitio web.

Lo novedoso de esto es el método para extraer los datos (como nombre, dirección, número de tarjeta, vencimiento y CVV), que se realiza a través de un mensaje instantáneo enviado a un canal privado de Telegram utilizando un ID de bot codificado en el código skimmer.

> *«El intercambio de datos fraudulentos se realiza a través de la API de Telegram, que publica los detalles del pago en un canal de chat. Esa información estaban previamente encriptada para dificultar la identificación»,* dijo Segura.

Al utilizar Telegram, los hackers ya no tienen que molestarse en configurar una infraestructura de comando y control separa para transmitir la información, ni arriesgarse a que los dominios sean bloqueados o eliminados por servicios anti malware.

> *«Defenderse contra esta variante de un ataque skimming es un poco más complicado ya que se basa en un servicio de comunicación legítimo. Obviamente, se podrían bloquear todas las conexiones a Telegram a nivel de red y aún así salirse con la suya»,* agregó el investigador.