Hot Sale: una oportunidad para consumidores, negocios y hackers

Ciudad de México, 26 de mayo de 2025.- El comercio electrónico en México crece a un ritmo sin precedentes y su valor ya supera los 33 mil millones de dólares. Eventos de ventas como Hot Sale son un motor clave de este crecimiento. Según la AMVO, a mitad de los usuarios de Internet en el país afirman haber comprado productos o servicios durante este evento.

Este crecimiento representa una oportunidad de negocio significativa, pero también un alto nivel de riesgo tanto para las empresas como para los consumidores. Cloudflare, la empresa líder en conectividad en la nube, explica que durante las temporadas de ventas impulsadas por descuentos como Hot Sale, ciertos desafíos son evidentes:

- **Gestión del alto tráfico:** Los picos de tráfico, muy por encima de los niveles normales, pueden provocar problemas de latencia o incluso hacer que las tiendas en línea colapsen.

- **Ciberseguridad:** Estos periodos son terreno fértil para ciberataques destinados a interrumpir servicios o realizar actividades fraudulentas.

Cloudflare explica que el colapso deliberado de sitios web a través de volúmenes de tráfico inusualmente altos, como parte de campañas maliciosas, ha alcanzado niveles alarmantes. El año pasado, se mitigaron aproximadamente 21.3 millones de ataques DDoS, lo que representa un aumento del 53% en comparación con el año anterior. En promedio, Cloudflare bloqueó 4,870 ataques DDoS por hora.

Esta estrategia de ataque, que busca saturar plataformas en línea con tráfico para volverlas inaccesibles, tiene mayor actividad durante eventos de ventas de alto volumen como Hot Sale. Cloudflare está detectando y mitigando los ataques DDoS más grandes registrados en el mundo. Esto ocurrió el mes pasado, en abril de 2025, cuando Cloudflare detectó y mitigó automáticamente el ataque DDoS más grande del mundo, que alcanzó los 6.5 Tbps.

Para hacer frente a estas amenazas, que pueden surgir en cualquier momento, las principales organizaciones en México están recurriendo a Cloudflare para obtener protección y velocidad, especialmente durante eventos como Hot Sale. Tal es el caso de Falabella; para este minorista, la velocidad de entrega de datos, el rendimiento del sitio y los tiempos de carga proporcionados por Cloudflare se traducen directamente en ventas. Informan que anteriormente, la purga de caché les tomaba alrededor de dos horas; hoy en día, toma solo entre 20 y 30 milisegundos, mejorando significativamente la experiencia del usuario.

En el ámbito de la ciberseguridad, un ejemplo claro es Bitso, la plataforma de criptomonedas más grande de América Latina. Bitso utiliza el Firewall de Aplicaciones Web (WAF), protección

contra DDoS y la Red de Entrega de Contenidos (CDN) de Cloudflare. Estas soluciones bloquean actualmente más de 7.5 millones de solicitudes maliciosas al sitio web de Bitso cada mes, según la empresa.

Otro caso es el de Naranja, un emisor de tarjetas de crédito en Argentina. En solo 72 horas, el WAF de Cloudflare bloqueó más de 730,000 intentos de ataque en cinco dominios de alto tráfico.

Además de estos casos, se anunció esta semana que Cloudflare participó en una operación conjunta con Microsoft para desmantelar la operación del malware Lumma Stealer (también conocido como LummaC2), una de las plataformas de Malware como Servicio (MaaS) más peligrosas que siguen activas hoy en día. Lumma estaba robando credenciales, billeteras de criptomonedas, cookies y otros datos sensibles de máquinas infectadas.

A medida que se acerca la próxima gran temporada de compras, la oportunidad es innegable —pero también lo es la necesidad de protección. Cloudflare enfatiza que contar con una plataforma integral de ciberseguridad y conectividad para mitigar amenazas y mantener un entorno seguro y sin errores es fundamental. Hacerlo puede marcar la diferencia entre un Hot Sale con ingresos récord y satisfacción del cliente, o un golpe directo a las finanzas y reputación de una empresa.

###