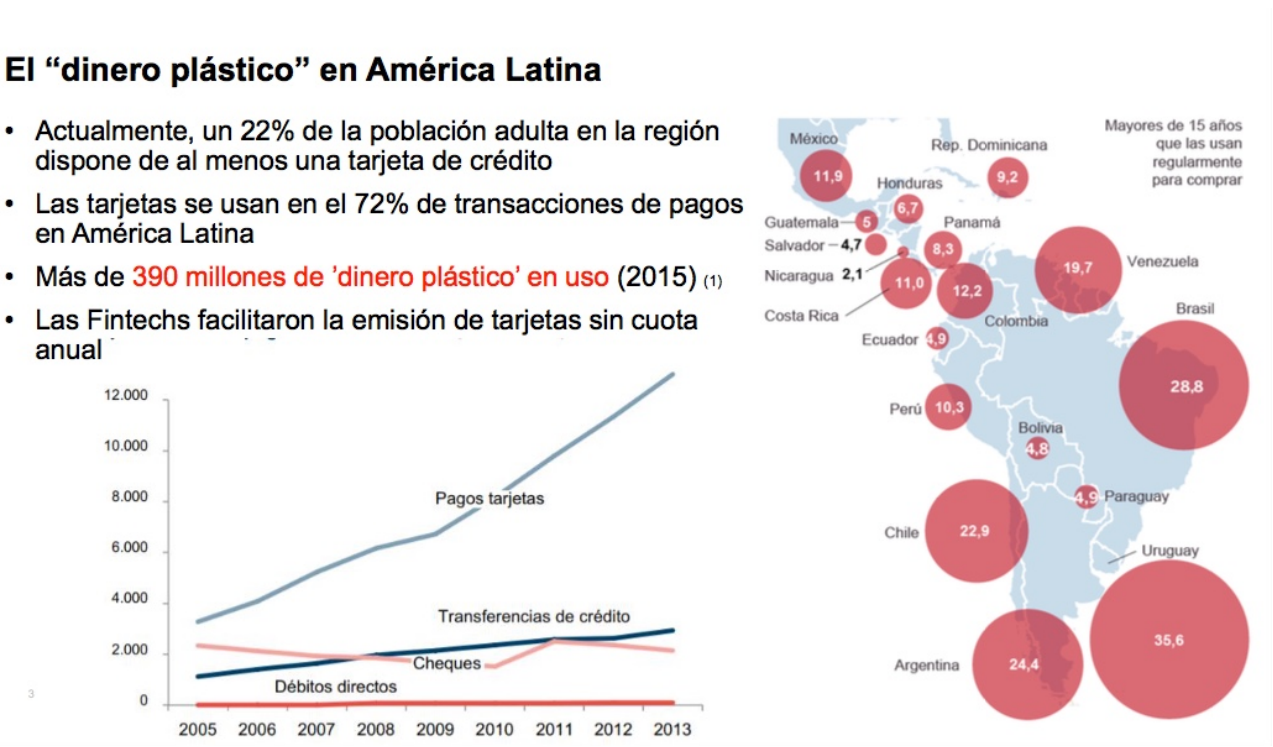
Aumenta la clonación a tarjetas de crédito en Latam

Kaspersky Lab ha registrado más de 1.000 ataques de malware en puntos de venta durante los primeros 8 meses del año en América Latina y destaca que es **Brasil quien ocupa el primer lugar en clonación de tarjetas de crédito en puntos de venta**, seguido por México y Ecuador, como recordaron los voceros de la empresa en la Séptima Conferencia Latinoamericana de Analistas de Seguridad que se celebra esta semana en Buenos Aires, Argentina.



Los investigadores desarrollaron a conocer cómo se desarrolla el malware dirigido a **Puntos de Venta** (POS) en América Latina, que tiene como objetivo **clonar tarjetas de crédito y débito**. Actualmente, concreta el informe de Kasperksy que "más del 22% de la población adulta en la región posee al menos una tarjeta de crédito, y 72% de las transacciones de pago de América Latina se hacen de esa forma".

Entre los años **2015 y 2016 sucedieron cerca de 1.300 ataques en puntos de venta en toda América Latina**. Los criminales que clonaron esas tarjetas utilizaron el malware **Dexter,** que es un código abierto disponible gratuitamente en Internet. Además, destaca que en tan solo los primeros ocho meses de 2017 se registraron 1.000 ataques, principalmente por el malware **NeutrinoPOS,** encontrado por primera vez en 2015 y que también se utiliza en ataques de denegación de servicio (DDoS).

De acuerdo con los investigadores de Kaspersky Lab, Brasil es el país líder en clonación de tarjetas en puntos de venta en América Latina, responsable de 77.37% de los ataques dedicados en la región. Seguido por México con cerca del 11.6% de los ataques a tarjetas.

El malware para punto de vent**a tiene funciones de "memory scraping" de la memoria RAM,**

que tiene como objetivo recoger datos importantes de la tarjeta, como los tracks 1 y 2. Los ataques a los puntos de venta ocurren desde 2005, cuando los delincuentes **usaban programas legítimos para interceptar el tráfico de la red de los PINPads** (dispositivo responsable de leer la tarjeta, donde el cliente digitaba el PIN). Antiguamente, la transferencia de información de estos dispositivos no estaba cifrada y, por lo tanto, era posible capturar la información enviada por los puertos USB con un software sniffer instalado en la computadora, obteniendo el Track 1 y Track 2 de las tarjetas, recuerdan los expertos en seguridad.

Kaspersky Lab aconseja que los bancos y comercios implementen todas las reglas PCI-DSS en sus máquinas buscando proteger la información y evitar ataques. Además, busquen e instalen una solución de seguridad completa en todos los equipos que estén conectados con el sistema de pagos.