Algunos cajeros automáticos que de la nada empezaron a *echar dinero*, fueron la clave para que las autoridades lograran desmantelar una red de delincuentes informáticos en México.

Esto ocurrió el pasado 3 de marzo en Guanajuato y Tijuana, después de que los cibercriminales faltaran a recoger los billetes de los cajeros.

En ese momento, la Agencia de Investigación Criminal de la Fiscalía General de la República ya seguía los pasos del grupo que hace llamar Bandidos Revolution Team.

Unos meses después, las autoridades procedieron al arresto del presunto líder, Héctor Ortiz Solares, conocido como H1 o «*Bandido Boss*», junto a siete cómplices.

En el operativo realizado el pasado 15 de mayo, también se incautaron diversos vehículos de lujo, computadoras, narcóticos, armas y cajas fuertes llenas de dinero en efectivo.

De este modo cayó el grupo de hackers detrás del mayor ataque cibernético en la historia de México. La mayoría de los implicados no pasaban de los 40 años y ya tenían la costumbre de sustraer mensualmente millones de pesos de los bancos del país.

Según los medios locales, las autoridades estiman que el grupo de hackers comenzó a operar hace unos cinco años. Pero fue un ataque específico realizado en abril del año pasado, el que puso en alerta a las autoridades.

Durante dicho ataque, los hackers manipularon el Sistema de Pagos Electrónicos Interbancarios del Banco de México (SPEI) para enviar dinero a distintas cuentas fraudulentas, para luego retirar el dinero por medio de cajeros automáticos.

Reuters reportó en ese entonces que el ataque le costó al sistema bancario mexicano entre 15 y 20 millones de dólares. Después, El Universal reportó que en realidad se documentaron 849 cuentas falsas, con un total de 500 millones de pesos, equivalente a más de 25 millones de dólares.

Los miembros de Bandidos Revolution Team siguieron accediendo al SPEI para obtener entre 100 y 300 millones de pesos cada mes.

Esto fue gracias a una combinación de talento y preparación con una arquitectura de red poco segura y debilidades en la supervisión de la seguridad del SPEI, según dijo un experto citado por Wired.

El Banco de México informó en agosto, que el ataque no tuvo como blanco a sus sistemas centrales, sino que estaba dirigido a interconexiones débiles o poco vigiladas.

También mencionó que la estrategia empleada por los ciberdelincuentes requería de *«un profundo conocimiento de la infraestructura tecnológica y los procesos de las instituciones víctimas, así como de acceso a estas».*

Por otro lado, también se acusa al grupo de haber cometido un ataque con ransomware a la aseguradora AXA, que le costó poco más de 1 millón de dólares.

Durante el cateo de las casas vinculadas a Ortiz Solares, se encontraron muchos productos de lujo adquiridos con tarjetas clonadas a distintos almacenes, y otros plásticos en proceso de clonación.

Finalmente, una fuente anónima contactó a las autoridades para denunciar que *«el cerebro del fraude al SPSE se llamaba Héctor y vivía en León»*, según reportó Héctor de Mauleón, periodista de El Universal.

Con esta información y las pistas recabadas por las autoridades, se llevó a cabo el arresto de los implicados, quienes fueron trasladados al penal federal de Almoloya de Juárez.