Clonar las tarjetas en puntos de venta o robar datos en línea para cometer fraudes cibernéticos ya no son las únicas herramientas de los ciberdelincuentes, firmas de seguridad digital detectaron que bandas utilizan métodos físicos para insertar virus en cajeros automáticos (ATM) para extraer dinero de forma ilegal.

Se trata del *software* pernicioso (*malware*) denominado Ploutus, cuya aplicación requiere cierto ingenio informático y capacidad física, descubierto en México el 13 de septiembre por la firma de seguridad Symantec.

El método de operación de Ploutus consiste en introducir un disco portátil (CD-Rom) con el virus al ATM. El *malware* se activará en unas 24 horas a partir de su inserción. Con ello, y de manera remota, los cibercriminales controlaran funciones como el dispensador de dinero y los menús: todo esto sin que se afecte el aspecto de la pantalla, de acuerdo con información de Symantec y de otras firmas de seguridad informática como Kaspersky Lab.

A diferencia de otro tipo de robos en cajeros ATM, el virus Ploutus sólo afecta a los bancos, y no a los cuentahabientes.

«Ploutus no utiliza los datos de una cuenta para sacar dinero del cajero. Su método de operación es acceder al sistema operativo del cajero y controlar ciertas funciones que le permiten al delincuente vaciarlo», explicó el analista de la firma de seguridad Symantec Geldarld Valle.

Sólo pasa en México…

Un reporte de BankInfoSecurity.com informa que Ploutus es un *malware* al parecer originado

en México. Como el programa requiere que se inserte de manera física en los ATM, los cajeros afectados no se ubican dentro de las sucursales bancarias o en lugares con mínimos niveles de seguridad.

CNNExpansión buscó un pronunciamiento de Bancomer, Banamex y HSBC, tres de los bancos con más cajeros automáticos desplegados en México. HSBC dijo que no cuenta con ningún cajero que pueda ser afectado por Ploutus.

La Comisión Nacional Bancaria y de Valores (CNBV) ya está tomando acciones en conjunto con la Asociación de Bancos de México (ABM) para poder tener un diagnóstico más preciso sobre el daño causado hasta el momento, así como las acciones que deben tomarse de manera inmediata y a corto plazo.

Aurelio Bueno, vocero de la CNBV, dijo que Ploutus «no representa ningún riesgo en el patrimonio de los clientes ni de clonación de tarjetas al realizar sus transacciones en cajeros automáticos».

El ejecutivo no dio datos de cuántos ATM han sido infectados pero la CNBV recomienda a los cuentahabientes reportar anomalías detectadas «utilizar, de preferencia, aquellos ubicados dentro de las sucursales».

Geldarld Valle, de Symantec, explicó que al ser necesario el contacto físico con el equipo para la activación del*malware*, podría haber colusión entre las empresas encargadas de administrar y dar mantenimiento a los cajeros automáticos y los *hackers*.

La construcción de este *malware* hace suponer que se creó en México o América Latina, puesto que está programado en español y algunas partes en inglés, pero con faltas gramaticales o de ortografía, agregó.

Fuente: cnnexpansion