Deloitte.

Hackeo en cajeros automáticos, lo que hay que saber

Por ***Marcelo Díaz***

Los cajeros automáticos, conocidos en la industria TIC como ATM's, son uno de los objetivos preferidos de los ciberdelicuentes. De hecho, según un reciente reporte de Kaspersky, los ciberataques a ATM's se mantendrán en el top 5 de dispositivos que serán objeto de los cibercriminales en los próximos años, causando más de 100 millones de dólares de pérdidas alrededor del mundo.

El propósito de estos ataques es la obtención de dinero o de información para posteriormente acceder a las cuentas y para ello existen diversas formas: desde el robo o asalto directo hasta la intervención de la máquina a través de hardware y software especializado. Si a ello se suma que muchas veces estos dispensadores no tienen la monitorización ni fiscalización adecuadas, que la configuración de su software falla, que no cuentan con los controles criptográficos correspondientes o que el diseño del proveedor es deficiente, entre muchas otras instancias, sin duda, los cajeros son una tentación para los ciberdelincuentes.

Entre los posibles ataques está la ejecución de un software malicioso no autorizado o malware que posibilita la intervención de la comunicación y el control del dispensador; así como de la información que fluye entre una tarjeta y la interfaz del chip del lector de tarjetas; del ATM para que la tarjeta no sea devuelta al cliente; o para enviar comandos de dispensado. También está la instalación de un aparato que capta la información de la banda magnética de la tarjeta y la manipulación de la dispensadora para que no entregue dinero y lo retenga, además de la instalación de un dispositivo para capturar la data de la tarjeta del cliente, entre muchos más.

Uno de los malware más conocidos es el Ploutus que permite vaciar los cajeros usando teclados externos adosados a la máquina o vía mensaje de texto, SMS. Otro bien conocido es Rufus hackea los cajeros que usan software antiguo o ya obsoleto como el Windows XP.

Por lo anterior es importante conocer algunos "síntomas" que delatarían la intervención, manipulación o infección de un cajero. Entre ellos: reinicios inesperados, registros de transacciones que no cuadran con el valor del efectivo aparentemente retirado, cerraduras forzadas o extraídas.

Así, es vital tomar medidas que puedan evitar y/o enfrentar estos ataques, como contar con alertas de intrusión de la apertura de los cajeros, cámaras de vigilancia, cifrado del disco duro, control de periféricos USB, protección de tráfico en línea, firewall para control de comunicaciones, uso de alguna plataforma antifraude que entregue información detallada en tiempo real, monitoreo del ATM en los parámetros inherentes al acceso a la CPU, ethical hacking y auditorías, por mencionar algunas.

A ello es necesario sumar la educación permanente de los usuarios, la implementación de protectores de teclado, tecnología anti skimming y el rediseño del lector de tarjetas (bezel), así como la videovigilancia, inspección y monitoreo rutinarios; además de mantener medidas a nivel de autorización, normativas, alertas de detección de fraudes y la comunicación permanente con el cliente para alertarlo, por ejemplo, vía SMS, de las operaciones de sus tarjetas. Evitar el hackeo a los cajeros automáticos se puede.