Artículos

Skimming

Mariano Corbino

El skimming (utilizar en secreto una pieza de equipo electrónico que registra los detalles de la tarjeta de crédito o débito con el fin de utilizarlos de forma ilegal). Este método es utilizado para robar la información personal almacenada en las tarjetas y al mismo tiempo se registra el número de PIN para acceder a la cuenta.

El método de skinning utiliza dos componentes separados para trabajar; por un lado el skimmer en sí, un lector de tarjetas se coloca sobre la ranura para tarjeta real de los cajeros automáticos que actúa cuando las personas deslizan la tarjeta en el cajero automático pero en realidad lo están haciendo a través del lector que ayuda a concretar la falsificación que en ese preciso momento escanea y almacena toda la información de la banda magnética.

Sin embargo como se mencionara recientemente, para tener acceso completo a la cuenta bancaria todavía es necesario contar con el número de PIN. Para obtener ese código se utilizan las cámaras que pueden colocarse escondidas tanto cerca o dentro de los cajeros automáticos, las cuales pueden obtener una visión clara del teclado y registrar todas las acciones realizadas sobre el mismo.

Algunos cajeros automáticos emplean esquemas de teclados falsos en lugar de cámaras para poder así capturar los números de PIN necesarios para luego operar las tarjetas. Al igual que los skimmers de tarjetas, los teclados falsos o líquidos se ajustan sobre la verdadera ranura de tarjeta del cajero automático, están diseñados para imitar el diseño del teclado y montarse perfectamente adaptándose casi a la perfección con el original.

ALGUNAS MODALIDADES DE SKIMMING

POSskimmingSwaps

El tipo más común de ataque de skimmingsuele ser cometido por empleados de la tienda donde usted compra habitualmente utilizando un dispositivo de mano que copia los

datos de titulares de tarjetas cuando se procesa la tarjeta del cliente. Una vez que obtiene los datos de la banda magnética estos son descargados en un dispositivo electrónico (PC, Tablet, Celular, etc). A partir de ahí, los datos de la tarjeta se duplican para crear las llamadas tarjetas "blancas". Es un tipo de maniobra bastante riesgosa para el delincuente debido que tiene que cambiar manualmente el dispositivo, generalmente es llevado adelante por criminales de que podríamos colocarlos en un nivel inferior.

Cajeros Automáticos

Los cajeros automáticos están comprometidos con los dispositivos de skimmingque se colocan sobre el lector de tarjetas del cajero automático. En algunos casos, otras partes de los cajeros automáticos están cubiertos, para disimular mejor el skimmer. El skimmer(nombre de la persona que roba los datos) puede depender de Bluetooth o tecnología celular para transmitir de forma remota datos de la tarjeta. Los estafadores a menudo duplican sus esfuerzos con la instalación de la cámara estenopeica (proviene del griego "stenosopaios" significa "provisto de un pequeño agujero")o pinhole en inglés que pueden colocarse en porta folletos, barras de luces, espejos o altavoces para recopilar datos de PIN medida que se introducen.

Jackpotting es una técnica que utiliza el malware para tomar el control de un cajero automático con el fin de tomar el control del dispensador de efectivo para obtener dinero;

Black Boxinges una variante Jackpotting donde el atacante utiliza su propia PC para comunicarse con el dispensador de efectivo para poder vulnerar el sistema y obtener dinero en efectivo;

Man-in-the-middlees una técnica para manipular la comunicación entre la PC y el sistema host de los cajeros automáticos en tiempo real de las transacciones o transferencias de datos y pueden, por ejemplo, retirardinero sin cargo de la cuenta de la tarjeta.

Pishing

El phishinges un ataque donde la víctima es engañada para dar un acceso al sistema asaltante al ser dirigida a un sitio web que pretende ser la de la institución financiera de la víctima. Este sitio web solicita a la víctima confiada a entrar en su número de cuenta, nombre de usuario, contraseña y otros datos de identificación personal. A pesar de que el sitio web es en realidad una falsificación, la víctima con frecuencia cumple con la petición porque el sitio parece ser legítimo - con los logotipos de bancos y avisos legales.

Malware

Un atacante también puede engañar a una víctima para que instaleun malware (abreviatura de software malicioso los más conocidos son Virus, Gusanos, Troyanos, Backdoor, Dialer, Keylogger. Adware, Exploit)en un sistema informático.

El malware se suele instalar disimuladamente después que la víctima es inducida a hacer clic en un archivo adjunto o enlace incluido en un mensaje de correo electrónico. Algunos tipos de malware pueden registrar las pulsaciones de teclado del usuario o capturas de pantalla de registro cada vez que una víctima intenta conectarse a un sitio web financiero específico e introduzca la información de cuenta.

Como se ha podido observar los métodos son variados a la hora de hacerse con los datos de las tarjetas de débito y crédito para luego ser utilizados por los propios ladrones o para ser vendidos a usuarios para poder ser utilizados para transacciones comerciales de todo tipo. Una de las medidas que parece al menos resguardar los datos con mayor eficiencia es el sistema EMV (Europay MasterCard VISA) que valida las operaciones gracias a la información almacenada en su chip.

Esta nueva tecnología permite que al insertar la tarjeta con chip en la terminal, esta, compruebe la validez de la tarjeta y se autentique, evaluando el riesgo a partir de parámetros que el emisor ha introducido en el chip, así como los de la compañía emisora de tarjetas que el distribuidor o el proveedor del terminal han introducido en nombre de esta entidad. La implementación del chip brinda mayor seguridad a las transacciones porque tramita la compra a través del chip dificultando la posible clonación de la misa a diferencia de la tarjeta con banda magnética que requiere que el usuario de la misma deba proporcionar su PIN.