Ataques de prueba de tarjeta

Los ataques de prueba de tarjeta están entre los fraudes más sofisticados practicados por criminales código-letrados en el espacio digital, donde las tarjetas de crédito y de débito son la presa. Empiezan solicitando información, que podría ser un depósito de números de tarjeta y nombres, almacenados en la hoja de cálculo, base de datos o en cualquier otro lugar vulnerable para los hackers. La palabra hacker es un poco anticuada en la nueva era digital de hurtos organizados. Imaginamos al hacker como un operador de préstamo en un cuarto oscuro, sin ventanas con tres pantallas de computadora en frente de él — No es por ser sexista, pero Rami Malek patentó la imagen de hacker con *Mr. Robot* — cuando en realidad es más que un espacio con números en una oficina que se aproxima a un call center, es la *vanguardia* de la moda criminal — La adrenalina del robo sin el estigma de violencia — un tipo de Robin Hood zeitgeist cuello blanco, pero más allá de la TV y del cine, es crimen organizado y guerra económica patrocinada por el estado. Viene a la mente Corea del Norte, no hay nada bueno en el robo de datos.

Cómo funciona

El propósito de los ataques de prueba de tarjeta es conocer si la tarjeta de crédito o débito, aunque es robada, funciona. ¿Puede ser usada? ¿Aún hay combustible en el tanque? ¿O ha sido reportada como robada y cancelada? La prueba es verídica. La información es de calidad — nombre, cuentas de asociado, balances, expiración— y esto ocurre en diferentes escalas, puede ser una tarjeta o una parte de la información de la tarjeta. Si es la segunda opción es más serio, un criminal profesional llama con la habilidad de codificar y hacer scripts, capaz de probar miles de tarjetas contra numerosas ventas en línea, pueden hacer esto muy rápido, incluso probar simultáneamente la información de un gran número de tarjetas. Muchos de los actores de esta profesión criminal pueden ir al otro extremo y trabajar en ciberseguridad, no queremos ponerlos en un pedestal, ni aplaudirles, pero en la guerra es mejor ver a tu enemigo como es y darle una consideración real. Sun Tzu, *El Arte de la Guerra*.

Acto uno: Obtención de datos

Todo empieza con obtener información, nada lujoso, métodos verdaderos — si algo no está roto no lo repares —violación de datos, dueños de negocios pequeños cooperando con crimen organizado para leer tarjetas y guardar la información, hackeando bases de datos para descargar reservas de información de tarjetas de crédito y débito.

Acto dos: Validar información

Una vez que una tanda de información es recopilada en forma de tarjeta de crédito o de débito, los operadores criminales utilizan herramientas de software y scripting para probar en línea los datos de la tarjeta robada. Imagina a un robot jugando con cientos de máquinas tragamonedas al mismo tiempo una y otra vez, esperando el repique de gane en cualquier número de máquinas. Así es como funciona, una sofisticada organización criminal puede operar vastas cantidades de números de tarjetas, fechas de expiración, Valores de Verificación de Tarjetas (CVV) y códigos de combinación, rápidamente hasta que acaben con las tarjetas y las descarten o invaliden, después otro gran lote es descargado en su sistema, esto es una infracción a escala de fabricación.

Acto tres: La pequeña compra

En el acto tres ellos tienen tarjetas válidas, esto significa que la información asociada con la tarjeta sigue siendo vigente y oficial, sin embargo, nuestros intrépidos criminales no saben si los datos están custodiados, lo que puede ser conceptualizado como líneas de cebo para atrapar ladrones. Luego prueban las tarjetas, pequeñas compras para empezar, con mucha inocuidad, estudian las circunstancias para ver si dispara alguna alarma. Algunas veces la tarjeta puede ser reportada como robada poco tiempo después de la filtración de datos. Este peligro ocupacional debe ser abordado por los ladrones. El método es empezar con un bajo volumen de transacciones.

Los ladrones digitales corren el riesgo

Bandidos digitales de más alto nivel llevan a cabo su negocio con cierto grado de manejo de riesgos, saben a qué se enfrentan y que los sistemas de seguridad están monitoreando constantemente. Utilizan servidores Proxy o suplantación de identidad IP para enmascarase a sí mismos u operar desde cuentas comprometidas, debemos ser conscientes de lo preparados que están para robar, su oficio es ilegal, pero lo hacen con un sorprendente nivel de profesionalismo, manejan el riesgo.

Una única transacción exitosa valida los datos robados, la tarjeta es buena. Y se mueven al siguiente eslabón de la cadena criminal, tienen opciones, la tarjeta verificada puede ser vendida en el mercado negro digital, o realizar transacciones más grandes, utilizarán la tarjeta y luego la tirarán no sin antes lograr su umbral de compras aceptable comparado con el riesgo, y ellos miden el riesgo. El nombre del juego para ellos es mantenerse fuera de prisión y no ser capturados, pueden ser muy disciplinados al respecto.

Pérdidas

Las pérdidas son sentidas tanto por el dueño de la tarjeta como por el dueño del negocio que es estafado, el dueño de la tarjeta pierde dinero, el vendedor pierde reputación. La última cosa que una compañía quiere es que se sepa públicamente que han sido hackeados y estafados con información y tarjetas fraudulentas, si piensas que el riesgo de reputación es exagerado, recuerda la violación de Yahoo en 2013, tomó cinco años averiguar la seriedad del asunto, no fue hasta 2017 que admitieron públicamente que los tres millones de cuentas registradas fueron afectadas. Estas cosas son difíciles de calcular, pero es seguro decir que Yahoo nunca se recuperó de este incidente del 2013.

Para luchar contras los ataques de prueba de tarjeta, deben participar tanto vendedores como clientes, ahora la seguridad es un básico y necesario componente de cualquier vendedor online, entre más grande el comercio, más dinero pondrá el dueño en la publicidad del nombre de su compañía y mayor el riesgo de daño de reputación si son afectados por bandidos digitales. Todo son dólares y centavos, malas relaciones públicas es como un presupuesto de publicidad inverso, el presupuesto de marketing no vale nada si la reputación de la compañía es afectada por pérdidas persistentes o intermitentes de conocimiento público.

La defensa es la ofensa

Entonces ¿Cómo peleas contra ellos? ¿Cómo te defiendes contra los ataques de prueba de tarjetas? Hay varios métodos probados y verdaderos —monitoreo de transacciones, revisión de velocidad, verificación de captcha, análisis de ubicación de IP y algoritmos de detección de fraudes.

Muchos de ellos combinados con el poder de aprendizaje autónomo (ML) e Inteligencia artificial (AI), por ejemplo, monitoreo de transacción, se convierte exponencialmente más efectivo por la eficiencia de ML y AI, el cual es capaz de detallar muchos más patrones de reconocimiento en el monitoreo de transacciones. El aprendizaje autónomo (ML) implica que la computadora está aprendiendo, por lo tanto, hasta cierto punto, empezará a enseñarse a sí misma cómo ser más experta en la búsqueda de anomalías en el monitoreo de transacciones. Esta innovación tecnológica incrementa la seguridad de los comerciantes y del titular de la tarjeta. Las antiguas herramientas —autenticación de dos factores, sistemas de verificación de direcciones, códigos de verificación de tarjeta y monitoreo de velocidad de transacción— son reformadas y fortalecidas por ML y AI, como las legiones de Grecia viniendo en ayuda de Leónidas y sus 300 espartanos, y no en un momento demasiado pronto, porque los ladrones están a nivel global 24 horas al día, los siete días de la semana.