LexisNexis®
RISK SOLUTIONS

CASO DE ÉXITO

LexisNexis® Risk Solutions ayuda a disminuir los ataques de programas maliciosos en una gran institución financiera, reduciendo pérdidas por fraude

La inteligencia de identidad digital LexisNexis® ThreatMetrix® detecta eventos de alto riesgo casi en tiempo real, sin afectar la experiencia del usuario

SINOPSIS

COMPAÑÍA

Una gran institución financiera

REQUISITOS

- Evitar ataques de ingeniería social dirigidos que usan software de acceso remoto para infiltrarse en cuentas de usuarios fiables.
- Frenar ataques de programas maliciosos.
- Restringir eventos fraudulentos en el inicio de sesión y pagos.
- Reducir pérdidas por fraude.

SOLUCIÓN

LexisNexis Risk Solutions implementó un sistema de elaboración de perfiles casi en tiempo real basados en comportamiento de la sesión en línea de principio a fin, incluyendo registros de cuentas, inicios de sesión, cambio de detalles y preferencias, navegación de la cuenta, creación de nuevos beneficiarios y perfilado de pago para detectar anomalías indicativas de programas maliciosos o usuario ilegítimo de software de acceso remoto. Esto detuvo drásticamente el fraude, a la vez que mantuvo una experiencia sin fricciones para los clientes fiables.

RESULTADO FINAL

- Los ataques de programas maliciosos dirigidos fueron detenidos en un breve lapso con cero falsos positivos.
- Los intentos de suplantación de identidad fueron detectados y bloqueados.
- Los ataques man-in-the-browser intentando embaucar a usuarios para revelar datos de identidad fueron detectados.
- El uso ilegítimo de software de acceso remoto usado para la apropiación fraudulenta de cuentas fue detectado.
- Ahorro de millones de dólares en fraudes todos los meses.

CASO DE ÉXITO

Resumen

Esta institución financiera ofrece un amplio rango de servicios que incluyen banca personal y comercial, seguros, finanzas corporativas y banca privada. La filosofía del banco se enfoca en cumplir de manera efectiva con las necesidades de los clientes y brindar un servicio excelente a todo nivel. Salvaguardar a los clientes contra el fraude y ofrecerles una experiencia en línea sin fricciones son imperativos comerciales clave.

Con LexisNexis® Risk Solutions, esta institución financiera puede:

- Identificar eventos con dispositivos que usan herramientas antidetección que intentan evitar las identificaciones del dispositivo al cambiar las versiones del navegador, complementos instalados en el navegador, tipo de sistema operativo, zona horaria, etc.
- Reconocer la presencia de un programa malicioso al analizar patrones de comportamiento o alteraciones de páginas web, rechazar eventos fraudulentos e identificar eventos sospechosos.
- Detectar troyanos de acceso remoto (RAT) que intenten robar información personal o engancharse a una sesión de inicio de sesión de usuarios legítimos.

Problema comercial

Esta institución financiera, como muchas otras, estaba siendo cada vez más el blanco de precisos ataques de ingeniería social, lo que a menudo condujo a los usuarios a instalar, inadvertidamente, un software de acceso remoto o programa malicioso. En ocasiones, estos ataques estaban pasando fuertes barreras de autenticación de dos factores porque estaban enganchándose a inicios de sesión completamente autenticadas, por ejemplo.

Cuando los clientes accedían al sitio web para iniciar una sesión en su cuenta bancaria, hacer un pago, cambiar una contraseña, etc., estos programas maliciosos intentaban monitorear dónde se hacía clic y los campos que tenían datos personales, incluidos nombre del cliente, número de cuenta, contraseñas y otros datos confidenciales.

Esta institución financiera necesitaba una sólida solución para el fraude que pudiese analizar los datos de eventos actuales y comparar con comportamientos históricos para distinguir de manera precisa el comportamiento anómalo casi en tiempo real. Dichos eventos que demostraban comportamiento anómalo podrían entonces ser identificados para su revisión o rechazados directamente en base al riesgo asociado.

CASO DE ÉXITO

Esta institución financiera necesitaba una sólida solución para el fraude que pudiese analizar los datos de eventos actuales y comparar con comportamientos históricos para distinguir de manera precisa el comportamiento anómalo casi en tiempo real.

Aprovechando el poder de la inteligencia global compartida para detectar eventos de alto riesgo casi en tiempo real

La mejor manera de abordar el cibercrimen organizado y complejo es usando el poder de una red global compartida. La red LexisNexis® Digital Identity Network® recopila y procesa inteligencia global compartida de millones de interacciones diarias de consumidores, incluidos inicios de sesión, pagos y solicitudes de nuevas cuentas. Aprovechando las capacidades de LexisNexis® ThreatMetrix® y usando la información de la red Digital Identity Network, LexisNexis® Risk Solutions es capaz de crear una identidad digital única para cada usuario al analizar las innumerables conexiones entre los dispositivos, ubicaciones e información personal anónima. El comportamiento que se desvía de esta identidad digital fiable puede identificarse de manera precisa casi en tiempo real, alertando a esta institución financiera de posibles fraudes. El comportamiento sospechoso puede detectarse e identificarse para su revisión, autenticación incremental o rechazo antes de procesar una transacción, minimizando la fricción para los usuarios fiables.

Con ThreatMetrix esta institución fue capaz de:

- Identificar comportamientos fiables y asociaciones para cada usuario (dispositivos, direcciones IP, ubicaciones, comportamiento de sesión y comportamiento de pago).
- Identificar cambios anómalos en el comportamiento para evitar fraude de pago, incluyendo identificar la presencia de software de acceso remoto y firmas de comportamiento de programas maliciosos.

- Identificar la presencia de redes de fraude persistentes al interrelacionarlas con inteligencia en cuentas mula conocidas o comportamiento fraudulento detectado en otro lado en la red de LexisNexis Risk Solutions.
- Identificar anomalías del comportamiento relacionadas con fraude con información privilegiada.

Características clave de la solución LexisNexis® ThreatMetrix®

- **La tecnología de identificación digital de página** puede detectar cualquier modificación de página, tal como componentes de HTML o JavaScript inyectados por programas maliciosos casi en tiempo real, protegiendo transacciones en línea.
- **La protección contra programas maliciosos** ayuda a las empresas a mitigar el riesgo de los programas maliciosos más sofisticados, reduciendo así el fraude. Esto incluye la protección contra man-in-the- browser (MITB), troyano de acceso remoto (RAT), ataques de bots de alta velocidad/frecuencia a ataques de baja velocidad y lentos que imitan el comportamiento de clientes legítimos, ransomware, intentos de inicio de sesión claves, etc.
- **La detección de programas maliciosos y reputación de aplicación** en el kit de desarrollo de software móvil (SDK) evalúa todas las aplicaciones instaladas en dispositivos Android y los verifica contra una base de datos de firmas líder en la industria de más de 15 millones de aplicaciones móviles. Las aplicaciones fiables y conocidas son validadas, mientras que las aplicaciones que contienen programas maliciosos o reputaciones sospechosas son identificadas casi en tiempo real.

- **La tecnología de señuelo (honeypot)** activa trampas para detectar modificaciones de páginas web no autorizadas en el navegador. La trampa de honeypot aparece en el programa malicioso como si un usuario estuviera navegando en el tipo de sitios web de alto valor que en general son objetivo del programa malicioso. Cuando el programa malicioso intenta atacarlo - al inyectar contenido web adicional tal como elementos de forma adicionales o diálogos emergentes que solicitan información personal - nuestro honeypot detecta esos cambios casi en tiempo real.
- **LexisNexis® Risk Solutions puede aumentar sus capacidades** al incorporar suministros de inteligencia de amenaza externa adicionales a través del centro de integración. El centro de integración permite que instituciones integren relevantes fuentes de datos de terceros y servicios de atención al cliente para proporcionar servicios de autenticación y verificación de identidad adicionales para transacciones de alto riesgo.

LexisNexis® RISK SOLUTIONS

Para mayor información visite:
risk.lexisnexis.com/fraude