White Paper

Cómo Aware Ayudó a un Importante Banco Brasileño a Mantenerse por Delante de los Cambiantes Vectores de Ataque Dirigidos a la Autenticación Facial

AWARE

781.687.0300 | sales@aware.com | www.aware.com

Aware es el principal proveedor mundial de productos y soluciones biométricas. Las soluciones de gestión y verificación de identidad de Aware son utilizados en servicios financieros, seguridad empresarial, atención médica, recursos humanos, identificación de ciudadanos, control de fronteras, cumplimento de la ley, defensa e inteligencia. La tecnología Aware líder en la industria ayuda a las organizaciones a recopilar, administrar, procesar y comparar imágenes y datos biométricos para la ayuda de identificación y autenticación.

Aun cuando las contraseñas siguen siendo el método de autenticación más común para las aplicaciones de servicios de banca en línea y servicios financieros móviles, también son muy propensas al uso indebido. Además, el desacuerdo creado por el proceso de restablecimiento de contraseña continúa siendo un verdadero punto problemático para los usuarios.

La autenticación facial es inherentemente más segura y eficaz para evitar que los defraudadores abran cuentas falsas para el lavado de dinero y roben dinero de otras personas, con el beneficio de mejorar la experiencia del usuario.

En los último años, el uso de la autenticación biométrica facial se ha vuelto considerablemente más precisa, rápida y resistente a las variables de entorno y usuario. Sin embargo, la realidad es que los bancos pueden seguir siendo atacados y saboteados si no se implementan la tecnología y los servicios de soporte adecuados. El tipo de ataque más común, a menudo conocido como un ataque de “suplantación” o ataque de presentación, posiblemente puede engañar a los sistemas de autenticación facial presentando un “artefacto facial” de un usuario legítimo, el cual puede generarse fácilmente a través de la fácil disponibilidad de imágenes y videos de personas en las redes sociales.

Con más del 60 por ciento de las filtraciones de datos debido a casos de contraseñas débiles o robadas, las instituciones están buscando alternativas más seguras como los datos biométricos. Sin embargo, con un cambio de autenticación mediante contraseña a autenticación biométrica suele surgir una escalada en los intentos de filtración.

Un ejemplo ilustrativo es el trabajo de Aware con el sistema de autenticación biométrica facial de un importante banco brasileño, el cual tuvo gran aceptación entre sus usuarios debido a su alta eficiencia y precisión. Sin embargo, el banco comenzó a notar casos de ataques de presentación y poco tiempo después, ataques de inyección, que estaban penetrando y evadiendo el componente de autenticación facial de su sistema de registro.

En este informe, descubriremos cómo la respuesta ultrarrápida de Aware para implementar un sistema de varios niveles de mejoras de seguridad tanto biométrica, como no biométrica, proporcionó múltiples líneas de defensa contra estos ataques.

El Problema del Banco

Como muchas empresas de servicios financieros líderes del sector, este importante banco estaba usando autenticación facial para ofrecer a sus clientes tanto seguridad máxima, como facilidad de uso.

De hecho, este banco tenía un sistema de autenticación biométrica facial establecido antes de comenzar su trabajo con Aware y anteriormente había sido blanco de delincuentes, usando fotografías de otras personas para engañar al sistema. En algunos casos, los atacantes robaban o usaban fotos o tarjetas de identificación de los cuentahabientes para crear cuentas fraudulentas. Como un primer paso, Aware trabajó con el banco para implementar la plataforma Knomi para la detección de prueba de vida, con el fin de garantizar que sólo las personas vivas pudieran abrir cuentas.

Los ataques de presentación generalmente implican la presentación de una copia de un usuario autorizado – como una imagen tomada de la tarjeta de identificación de alguien o incluso un perfil en redes sociales – a una cámara u otro dispositivo de creación de imágenes. El objetivo del hacker o un usuario no autorizado es engañar al dispositivo para que piense que está verificando el rostro de la persona autorizada, de modo que puedan tener acceso de manera fraudulenta.

Sin embargo, con el paso del tiempo, la sofisticación de estos ataques de presentación siguió aumentando. En lugar de usar fotos para abrir cuentas fraudulentas, los defraudadores comenzaron a producir ataques de presentación de mayor calidad, así como deepfakes y transformaciones.

Los ataques de presentación más sofisticados implican máscaras en vez de una foto. Un atacante podría recortar los ojos de una fotografía y presentar su rostro al dispositivo de creación de imágenes o incluso fabricar una máscara tridimensional específicamente para este propósito. El objetivo aquí es asegurarse de que la vivacidad de los ojos y/o la calidad de las máscaras den al delincuente una ventaja para pasar el punto de control biométrico.

Y después, hace aproximadamente nueve meses, el banco empezó a ver un tipo de ataque diferente: ataques de inyección, destinados a evadir el sistema de registro de los clientes. Los ataques de inyección representaron un vector de ataque completamente diferente a los ataques de presentación del mundo real que el banco había experimentado en un principio. En lugar de atacar la presentación del usuario y los algoritmos que analizan esa presentación, atacaron el software que realiza la captura en sí.

Las vulnerabilidades de inyección permiten a los atacantes introducir datos maliciosos en, o relacionar un código malicioso a través de, una aplicación en otro sistema. Durante un ataque de inyección, los datos no confiables o el código no autorizado son inyectados en un programa, donde se interpretan como parte de una consulta o un comando. El programa se altera entonces y esa alteración redirige el programa para un propósito mal intencionado.

Los ataques de inyección son particularmente alarmantes porque la superficie del ataque es enorme y el ataque puede tocar un sistema completo. Los ataques de inyección son también una clase de vulnerabilidad sumamente bien entendida, lo que significa que hay muchos recursos y herramientas de fácil acceso que permiten a los atacantes, incluso sin experiencia, sacar provecho de esas vulnerabilidades.

La Solución de Aware

Aware implementó tres niveles de protección adicional para frustrar los intentos de evadir el componente de autenticación facial del sistema de registro del banco. El primer nivel fue asegurar la aplicación, de tal modo que se mantenga la integridad del proceso de captura biométrica. El segundo nivel fue el análisis de los datos biométricos para los ataques de presentación.

El tercer nivel se basó en las mejores prácticas de no biometría para verificar la seguridad de los datos biométricos de los usuarios en cada uno de los siguientes pasos. Aware abordó los aspectos de seguridad de todas estas partes diferentes del proceso de incorporación, aunque técnicamente no correspondían al alcance de trabajo de la compañía e incluye:

- **Adquisición de datos:**
  El momento en que el dispositivo acepta los datos de un usuario.
- **Seguridad en la transferencia de datos:**
  Garantizar que los datos del usuario sean codificados y transferidos a donde serán procesados.
- **Procesamiento de datos:**
  Mantener los datos codificados y seguros hasta que sean devueltos con la respuesta.

Como resultado de las medidas implementadas por Aware, el banco observó inmediatamente una disminución significativa en el vector de ataque de inyección.

Mejores Prácticas y Aprendizajes

Existen varios aprendizajes del trabajo de Aware con este banco, que otros deberían considerar cuando se enfrenten a los cambiantes vectores de ataque de la autenticación biométrica:

Enfoque Integral de la Autenticación Biométrica:

La Detección de Ataques de Presentación (PAD por sus siglas en inglés) es un componente crítico, pero sólo un elemento en un complejo sistema de autenticación biométrica, que necesita proporcionar un equilibrio cuidadoso entre la seguridad y la utilidad. Una solución exitosa debe ofrecer un conjunto completo de defensas que minimice el desacuerdo, pero maximice la probabilidad de un resultado preciso y uno que pueda adaptarse a las nuevas amenazas.

Esto incluye:

1. Un método eficaz para el control de calidad, que motiva a los usuarios a optimizar su presentación para el análisis más preciso, proporcionado por la excepcional capacidad de captura automática de Aware
2. Una serie primaria de sofisticados algoritmos de PAD, para detectar ataques de presentación incluso antes de que entren al subsistema biométrico, proporcionada como parte de la plataforma Knomi, la solución líder de prueba de vida de Aware
3. Una serie secundaria de sofisticados algoritmos de detección de ataques informáticos, para proteger el sistema de ataques de emulación, inyección y función que podrían incluir deepfakes, transformaciones o replicación de datos
4. Un método seguro de extremo a extremo, que verifica la integridad de toda la transacción
5. Por último, una infraestructura de diseño de soluciones que permita un enfoque altamente receptivo y adaptable de las amenazas en constante evolución, cuyo éxito se refleja hoy en día en la posición de liderazgo de Aware en la autenticación biométrica

Las medidas de seguridad institucionales adicionales como monitorear los identificadores de dispositivos (o direcciones IP) que estén asociados con transacciones, frecuentemente rechazadas, memorizar el número de cuentas diferentes a las cuales se tiene acceso con el mismo identificador de dispositivo (o direcciones IP) y/o usar comparadores para verificar las identidades de los cuentahabientes, todas pueden contribuir a asegurar las transacciones financieras que deseen, para aprovechar al máximo la tecnología de la autenticación biométrica.

En este sentido, la importancia de colaborar activamente con las instituciones participantes no puede ser subestimada, ya que luchar por el objetivo común de una autenticación facial altamente precisa y segura, puede ofrecer oportunidades de sinergia para progresar en los últimos avances. Aware se distingue por entablar y cuidar las relaciones que pueden ser mutuamente beneficas, necesarias para tener éxito en el entorno complejo y dinámico de la autenticación biométrica.

Aprender de las Realidades Operativas:

Es fácil describir lo que teóricamente se puede hacer en el caso de un ataque de la autenticación biométrica, pero eso es muy diferente a aplicar soluciones en el mundo real y en tiempo real. Al trabajar con este banco, Aware pudo acceder a estos vectores de ataque y aplicar medidas de protección de manera directa y extremadamente rápida.

Además, Aware pudo mejorar la eficacia y precisión de sus algoritmos basándose en los datos sobre los vectores de ataque proporcionados por el banco. Esta relación de sinergia benefició tanto a los esfuerzos de Aware, como al trabajo de seguridad del banco, a medida que los vectores de ataque evolucionaron.

Equilibrar la Seguridad y la Utilidad:

Abordar asuntos de seguridad complejos y maximizar la utilidad del sistema puede ser un equilibrio difícil de lograr. La mayoría de los bancos reconocen la necesidad de hacer concesiones entre la comodidad y la seguridad de los clientes, de hecho, muchos lo ven sólo como el costo de hacer negocios. Como un ejemplo, VISA cancela una cifra estimada de $6 mil millones de dólares en fraudes al año para mantener sus sistemas de autenticación fáciles de usar.

En otro ejemplo, muchos bancos implementan mecanismos de protección adicionales como funciones de concordancia. Esto es cuando, una vez que una persona haya accedido a una cuenta, un motor de concordancia continuamente compara la imagen facial del usuario con la imagen del cuentahabiente archivada. El umbral de concordancia en muchos bancos es muy poco severo, tanto que incluso si un usurpador logra pasar el punto de control inicial de la autenticación, el motor de concordancia sigue sin determinar que el usurpador no es el cuentahabiente. Esto se hace específicamente para garantizar una experiencia sencilla para los usuarios legítimos.

La conclusión es que, cuando se implementan medidas de protección de seguridad, la utilidad debe ser valorada tanto como el aspecto de la seguridad. Afortunadamente, Aware proporcionó al banco la capacidad de captura automática interactiva, lo que ofreció oportunidades para tener un efecto directo y positivo en la utilidad.

Garantizar una Alianza de Calidad:

Aware da prioridad a verdaderas alianzas con sus clientes, especialmente en esta era digital, con ciberataques cada vez más frecuentes y más malicia. Esto es particularmente cierto en Brasil, que experimentó un enorme aumento en las interacciones en dispositivos móviles como consecuencia de la COVID-19 y, a su vez, un gran incremento en los vectores de ataque más agresivos.

La estrecha alianza de Aware con este banco—una que implicó la cooperación tanto a nivel de seguridad técnica, como a nivel de seguridad empresarial y el intercambio de datos de transacciones—fue uno de los componentes clave para una colaboración exitosa y que ha permitido al banco mantenerse por delante de los cambiantes vectores de ataque, con el fin de obtener todos los beneficios de su inversión en la autenticación biométrica.

Resumen

Las contraseñas siguen siendo el método de autenticación más común para la mayoría de las aplicaciones de servicios de banca en línea y servicios financieros móviles, pero son propensas al uso indebido y el proceso de restablecimiento de contraseña continúa siendo un punto de gran frustración para los usuarios. A medida que los bancos aumentan su receptividad a tecnologías de autenticación biométrica más modernas, necesitan colaborar con sus socios de tecnología para estar un paso adelante de las amenazas emergentes.

Aware proporcionó a este banco orientación tanto dentro, como fuera del ámbito de la seguridad biométrica y logró un alto grado de éxito. Aware hará lo que sea necesario para ayudar, ya que nada es más importante para la compañía que proteger los activos confidenciales y valiosos de sus clientes empresariales y sus usuarios de amenazas perniciosas.

Este tipo de alianza es esencial para el futuro de la seguridad biométrica, especialmente en el mundo de la banca y la tecnología financiera. A medida que estas organizaciones continúen evaluando la autenticación biométrica, es fundamental que consideren firmemente la elección de un socio y la mayoría se beneficiará de uno comprometido con la comunicación constante y la capacidad de respuesta proactiva en tiempo real a las amenazas. Trabajando juntos, el socio de tecnología correcto puede ayudar a las organizaciones a lograr los beneficios máximos de la autenticación biométrica - seguridad superior combinada con la mayor comodidad que mantenga a los usuarios leales a la marca.

¿La interesa saber más? Visite www.aware.com

AWARE

781.687.0300 | sales@aware.com | www.aware.com