KASPERSKY FRAUD PREVENTION - CLIENTLESS ENGINE

Seguridad más inteligente = una mejor banca digital

Mientras las instituciones financieras se apresuran para poder ofrecer a sus clientes la experiencia de banca en línea más intuitiva y satisfactoria, los cibercriminales profesionales se apresuran a desarrollar malware cada vez más sofisticado para sacar el máximo provecho de cada nueva oportunidad para cometer fraudes en línea.

Las nuevas y poderosas técnicas de ataque que tal vez ya haya experimentado incluyen:

- **Infiltración de página web** - campos adicionales que se "inyectan" en su página de inicio de sesión y que capturan datos confidenciales del cliente como el número CVS de la tarjeta, para usarlos en ataques "sin la tarjeta".
- **Ventanas emergentes falsas (phishing)** - adición de una petición "emergente" del hacker para obtener datos adicionales, por ejemplo, un número de teléfono celular, para poder interceptar verificaciones de 2 factores.
- **Manipulación de transacciones** - por ejemplo, pedir a los clientes que "paguen" dinero ingresado falsamente por error en su cuenta, o hacer una transacción "de prueba" para ayudar al banco.

Todas estas técnicas comienzan con la instalación de malware, por lo general en forma de troyanos bancarios, en su sistema de banca en línea. Y este malware suele introducirse por el punto más vulnerable de su sistema: sus clientes. Los atacantes comienzan infectando el dispositivo de su cliente, y luego utilizan la conexión en línea a su sistema como punto de entrada.

¿Cómo puede protegerse de los complejos ataques de fraude que se inician en dispositivos del usuario infectados, sin afectar la experiencia relajada y sin complicaciones de banca en línea que hace que sus clientes estén satisfechos y sean leales?

Kaspersky Fraud Prevention Clientless Engine evita que los cibercriminales lancen ataques exitosos mediante:

Detección del malware financiero:
La búsqueda e identificación proactivas de malware que intenta infectar sus páginas web a través de los dispositivos de sus clientes.

La detección de cualquier computadora o teléfono celular infectados que intenten iniciar actividades maliciosas a través de la conexión en línea a su sitio, sin que esto tenga un impacto en los clientes no infectados o en su experiencia de banca digital.

Informes integrales:
Alertas para que su banco pueda tomar medidas, que pueden incluir:
- El bloqueo de la transacción
- La terminación de la sesión del usuario
- El manejo del caso del cliente para garantizar que el incidente no se repita.

Administración de endpoint:
Le proporciona datos de incidentes a través de la consola de Kaspersky Fraud Prevention, que se envían a sistemas internos o de terceros para su análisis e investigación posteriores, si fuera necesario.

Fuentes de inteligencia:
Les proporciona a sus equipos de administración de banca en línea la información que necesitan para tomar decisiones de seguridad complejas.

Aunque usted tiene visibilidad de cada incidente potencial, el proceso es transparente para los usuarios, a menos que su dispositivo esté infectado con malware bancario. En este caso, usted podrá tranquilizarlos y asesorarlos sobre cómo mantenerse seguros en el futuro.

El resultado es un ambiente de banca en línea más seguro para todos, que le brinda la oportunidad de ganar y retener más clientes y desarrollar aún más la funcionalidad de su portal de banca digital sin que aumente el riesgo de intentos de fraude no detectados.

Contáctenos para obtener más información: KFP@kaspersky.com
http://www.kaspersky.com/business-security/fraud-prevention

Kaspersky Fraud Prevention Clientless Engine, hoja de información, agosto de 2015 GL