



DOTLAKE EN LA INDUSTRIA FINANCIERA

Whitepaper

LAS AMENAZAS CIBERNÉTICAS EN LAS INDUSTRIAS FINANCIERA Y DE SEGUROS SON CADA VEZ MÁS PELIGROSAS, CON ACTORES SOFISTICADOS QUE EXPLOTAN LAS DEBILIDADES Y VULNERABILIDADES.

Las **industrias bancaria y de seguros** se han vuelto más dependientes de las soluciones digitales, exponiéndose a **nuevos riesgos cibernéticos**. Los ataques cibernéticos son cada vez más sofisticados, orquestados por estructuras criminales organizadas que comparten información en sitios y foros oscuros. Las instituciones financieras son vulnerables debido a su **dependencia de productos y servicios de terceros**, lo que genera riesgos sistémicos en múltiples entidades. Además, la adopción de big data y análisis avanzado presenta desafíos adicionales, ya que los ciberdelincuentes emplean técnicas avanzadas como la ingeniería social para apuntar al sector. Los incidentes cibernéticos pueden tener graves consecuencias, incluidas interrupciones comerciales, pérdidas financieras y daños a la confianza del cliente.

Iniciativas recientes como la Ley de Resiliencia Operacional Digital, o **DORA**, y otras en este campo requerirán monitorear de cerca los nuevos riesgos para anticipar la aparición de nuevas amenazas cibernéticas para la protección del cliente. Todo esto hace que las entidades financieras se adapten rápidamente a soluciones actualizadas y obtengan un conocimiento más profundo del contexto ciberdelincuente.

De acuerdo con esto, las instituciones financieras deben anticiparse a las amenazas cibernéticas y agregar un monitoreo en tiempo real de datos especializados de las fuentes usadas por los ciberdelincuentes.

¿Cómo **DOTLAKE** puede ayudarte?

- Obtenga acceso a través de API a información procesable de la web profunda, redes oscuras, sitios de rescate y foros más relevantes de ciberdelincuentes para ser consumida de una manera fácil, segura y rápida de acuerdo con sus necesidades específicas y casos de uso.
- Detección en tiempo real: para identificar menciones en una etapa temprana obteniendo una visión más amplia del contexto y la gravedad de una amenaza potencial.
- Recepción de alertas: puedes configurar alertas tempranas de acuerdo con sus prioridades relacionadas con los activos, productos, credenciales y su marca. Reduzca el ruido de la red y el número de incidentes no relevantes para su negocio.
- Plataforma: Acceso a nuestra web donde podrá realizar un análisis más granular de los riesgos y amenazas para su empresa.
- Fácil integración de la información en sus plataformas de gestión de ciberseguridad, SOC y sistemas.

Según VMware, la primera mitad de 2020 vio un **aumento del 238 %** en los ataques cibernéticos dirigidos a **instituciones financieras**. Y según IBM, el coste medio de una filtración de datos en el sector financiero en 2021 es de **5,72 millones** de dólares.

Si bien los proveedores de servicios financieros poseen principalmente datos financieros confidenciales, los grupos de seguros son un objetivo natural para los ataques cibernéticos porque poseen cantidades sustanciales de información confidencial de los asegurados (registros médicos, etc.). Los datos obtenidos pueden utilizarse para diferentes fines delictivos, como el **robo de identidad** para obtener ganancias financieras.

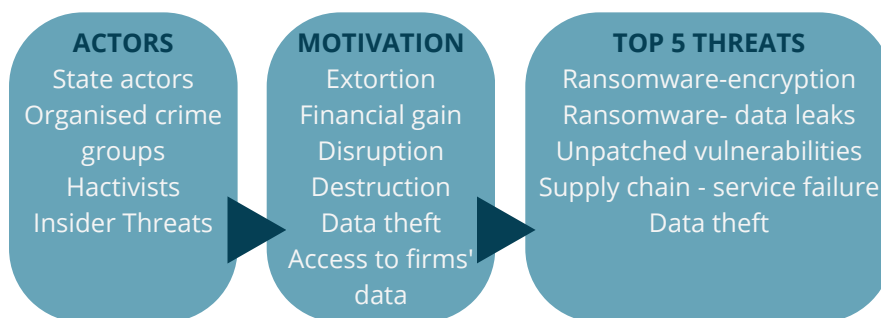
Según Accenture, una organización de seguros típica se enfrenta más de tres ataques efectivos por mes, sin embargo, cuatro quintas partes de los ejecutivos de seguridad de las aseguradoras más grandes confiaban en sus estrategias de ciberseguridad. Si bien, en otro informe de EY, casi la mitad de las aseguradoras han descubierto incidentes de ciberseguridad "significativos" dentro de su organización.

Ha habido varias infracciones de alto perfil en los últimos años. A principios de 2015, Anthem, la segunda aseguradora de salud más grande de los EE. UU., extrajo hasta 80 millones de registros de clientes y empleados. Según EY, se espera que el impacto financiero supere su política de ciberseguridad, cubriendo pérdidas de hasta \$100 millones.

Se robó la PII de 11 millones de clientes de Primera Blue Cross y se anunció en marzo de 2015, lo que tuvo un impacto legal y reputacional muy negativo en la aseguradora. Al enfatizar la importancia de la violación, recientemente se supo que la aseguradora destruyó intencionalmente la evidencia en el caso a pesar de los litigios en curso en su contra, varios años después.

Los ataques de ransomware son cada vez más sofisticados y dañinos, lo que a su vez puede permitir que los actores de amenazas de ransomware obtengan aún más recursos. **2022 fue uno de los años más activos para la actividad de ransomware.**

EL PANORAMA DE LAS CIBERAMENAZAS PARA LAS INFRAESTRUCTURAS DE LOS MERCADOS FINANCIEROS EN EUROPA



Nota: Las amenazas están organizadas en orden descendente de gravedad estimada

Con DOTLAKE también podrás:

- **Acceder a sitios de ransomware altamente especializados** para comprender cómo actúan los ciberdelincuentes en este campo y cómo anticipar posibles próximos ataques bajo planificación.
- Obtener una visión directa más compleja de su **Gestión de riesgos de terceros (TPRM)** para identificar vulnerabilidades de seguridad derivadas de sus socios externos.
- Mejorar sus soluciones de gestión de superficie de ataque aumentando su capacidad de **detección de fugas de datos** que pueden reducir significativamente las posibilidades de una filtración de datos exitosa.
- **Investigar TTP** (tácticas, técnicas y procedimientos): los actores de amenazas a menudo usan estrategias de ataque similares debido a vulnerabilidades similares en toda la industria. Con DOTLAKE estarás informado de los últimos TTP que están siendo utilizados por los ciberdelincuentes.
- Obtener un mejor control a través de la **vigilancia digital** de sus activos clave, incluidos sus proveedores externos, para reducir el riesgo en su contexto comercial y cadena de valor.
- Vigilar más de cerca su sector y el contexto de la industria para **mejorar sus decisiones de ciberseguridad**.

CONCLUSIÓN

Los sectores financiero y de seguros son cada vez más objeto de ciberataques a medida que adoptan la digitalización y amplían su presencia digital. Estos ataques plantean riesgos sistémicos, ya que los actores de amenazas explotan las vulnerabilidades en los sistemas de terceros en los que confían varias entidades. Los ataques de ransomware, en particular, se han convertido en un desafío importante, causando grandes pérdidas financieras.

El auge de las empresas Fintech e Insurtech, si bien es beneficioso para la eficiencia y la inclusión de la industria, también la ha expuesto a mayores riesgos cibernéticos. Además, Los ciberdelincuentes se han convertido en organizaciones profesionales que utilizan foros, mercados y redes especializados para compartir información y ejecutar sus actividades delictivas.

Para combatir eficazmente estas amenazas cibernéticas, los analistas de seguridad cibernética requieren **acceso a datos calificados de fuentes criminales** donde ocurren estas actividades. Al aprovechar la inteligencia cibernética, los analistas pueden anticipar ataques potenciales, evaluar el nivel de compromiso y optimizar los recursos de seguridad cibernética al priorizar amenazas reales e inminentes.

Es crucial que las instituciones financieras y de seguros se **mantengan alerta e inviertan en medidas robustas de ciberseguridad**, incluyendo monitoreo continuo de ciberdelincuentes, detección oportuna de amenazas. Al priorizar la ciberseguridad y ciberinteligencia puedes proteger mejor sus operaciones, los datos de los clientes y mantener la confianza de sus partes interesadas.