DOTLAKE

DOTLAKE IN FINANCIAL INDUSTRY

Whitepaper

CYBER THREATS IN THE FINANCIAL AND INSURANCE INDUSTRIES ARE INCREASINGLY DANGEROUS, WITH SOPHISTICATED ACTORS EXPLOITING WEAKNESSES AND VULNERABILITIES.

The **banking and insurance industries** have become more reliant on digital solutions, exposing themselves to new cyber risks. **Cyber-attacks** are becoming **more sophisticated**, orchestrated by organized criminal structures that share information on dark sites and forums. Financial institutions are vulnerable due to their reliance on **third-party products** and services, leading to systemic risks across multiple entities. Furthermore, the adoption of **big data and advanced analytics** introduces **additional challenges**, as cyber-criminals employ advanced techniques like social engineering to target the sector. Cyber incidents can have severe consequences, including business interruptions, financial losses, legal fees, and damage to customer trust.

Recent initiatives such as the Digital Operational Resilience Act, or DORA, and others in this field will require close monitor new risks to anticipate the emergence of new cyber threats for the customer's protection. All this makes financial institutions quickly adapt to updated solutions and get a deeper knowledge of the cyber-criminal context.

According to this, financial institutions need to anticipate cyber threats and potential successful breaches by adding critical real-time monitoring of critical sources of information from specialized data criminal network environments where cyber criminals interact.

How **DOTLAKE** can help?

- Get access through API to actionable information from the deep web, darknets, ransomsites, and cybercriminal most relevant forums to be consumed in an easy, safe, and quick way according to your specific needs and use cases.
- Real-time detection: to detect mentions in an early stage getting a wider vision of the context and severity of a potential threat.
- Be focused. Receive alerts: to receive early alerts according to your priorities related to the assets, products, credentials, and your brand. Reduce the network noise and number of non-relevant incidents for your business.
- High visualization: Access to a playground where you will be able to do a more granular analysis of the risks and threats for your company.
- Easy integration of the information in your cybersecurity management platforms, SOCs, and systems.

DOTLAKE

According to VMware the first half of 2020 saw a 238% increase in Cyberattacks targeting financial institutions. And according to IBM, the average cost of a data breach in the financial sector in 2021 is $5.72 million.

While financial services providers hold mainly sensitive financial data, Insurance groups are a natural target for cyber-attacks because they possess substantial amounts of confidential policyholder sensitive information (medical records,..). Data obtained can be used for different criminal purposes such as identity theft to obtain financial gains.

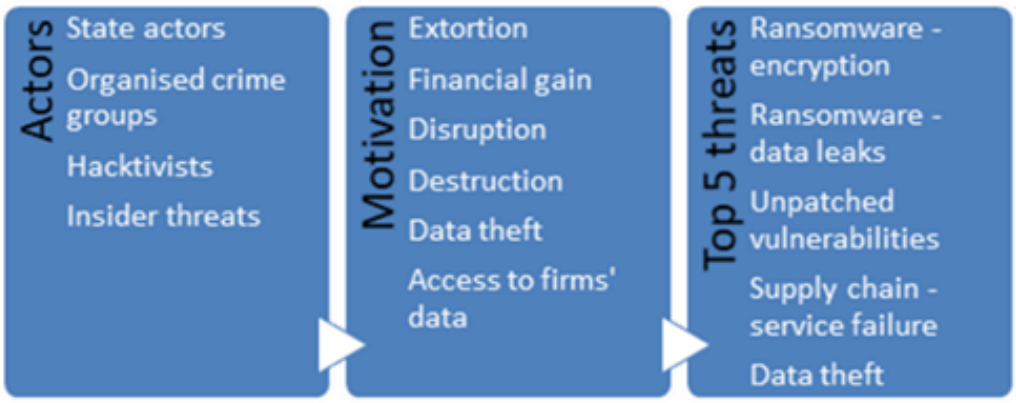
According to Accenture, a typical insurance organization faces more than three effective attacks per month, yet four-fifths of the larger insurers' security executives were confident in their cybersecurity strategies. Yet in another report from EY, almost half of the insurers have discovered "significant" cybersecurity incidents within their organization.

There have been several high-profile breaches in recent years. In early 2015, Anthem, the second-largest health insurer in the US, had up to 80 million customer and employee records exfiltrated. According to EY, the financial impact is expected to surpass its cybersecurity policy, covering losses of up to $100 million.

11 million customers' PII was stolen from Premera Blue Cross and was announced in March 2015, which had a hugely negative reputational and legal impact on the insurer. Emphasizing the significance of the breach, it has only recently emerged that the insurer intentionally destroyed evidence in the case despite ongoing litigation against it, several years down the line.

Ransomware attacks are growing more sophisticated and damaging, which in turn may enable ransomware threat actors to obtain even more resources. 2022 was one of the most active years for ransomware activity

The cyber threat landscape for financial market infrastructures in Europe



Note: Threats are arranged in descending order of estimated severity

With DOTLAKE you will also can:

- Access to **highly specialized ransomware sites** to understand how cybercriminals are acting in this field and how to anticipate potential next attacks under planning.
- Get a direct more complex vision of your **Third-Party Risk Management (TPRM)** to identify security vulnerabilities derived from your third-party partners.
- You can improve your Attack Surface Management solutions increasing your capacity of **detecting data leaks** that can significantly reduce the chances of a successful data breach.
- **Learn TTP** (Tactics, Techniques, & Procedures) - Threat actors often use similar attack strategies due to similar vulnerabilities across the industry. With DOTLAKE you will be informed of the last TTPs that are being used by cybercriminals.
- Get better control through the **digital surveillance** of your key assets including your third-party providers to reduce the risk in your business context and value chain.
- Keep a closer eye on your sector and industry context to **improve your cybersecurity decisions**. Get an alert to detect when the key actors and players in your industry to anticipate how this can affect your company.

CONCLUSION

The financial and insurance sectors are increasingly targeted by cyber-attacks as they embrace digitalization and expand their digital presence. These attacks pose systemic risks, as threat actors exploit vulnerabilities in third-party systems that multiple entities rely on. Ransomware attacks, in particular, have emerged as a significant challenge, causing financial losses and disrupting operations.

The rise of Fintech and Insurtech firms, while beneficial for the industry's efficiency and inclusivity, has also exposed it to greater cyber risks. Moreover, geopolitical tensions have further fueled cyber-attacks in the sector. Cybercriminals have evolved into professional organizations, utilizing specialized forums, markets, and networks to share information and execute their criminal activities.

To effectively combat these cyber threats, cybersecurity analysts require **access to qualified data** from criminal sources where these activities occur. By leveraging cyber intelligence, analysts can anticipate potential attacks, assess the level of compromise, and optimize cybersecurity resources by prioritizing real and imminent threats.

It is crucial for financial and insurance institutions to **stay vigilant** and invest in robust cybersecurity measures. This includes ongoing monitoring of cybercriminal networks, timely threat detection, and proactive incident response strategies. By prioritizing cybersecurity and leveraging cyber intelligence, these sectors can better protect their operations, customer data, and maintain the trust of their stakeholders.