Trend Micro Highlights Security Risks of New Open Banking Regulation

FinTech changes could open up new attacks on organizations and consumers

DALLAS, September 17, 2019 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today release research demonstrating that major new European banking rules could greatly increase the cyberattack surface for financial services firms and their customers.

The new research details the impact of the EU's Revised Payment Services Directive (PSD2), which is designed to give users greater control over their financial data and the option of sharing it with a new breed of innovative Financial Technology (FinTech) firms. The same ideas are spreading globally under the term "Open Banking."

"The financial sector has always been a highly attractive target for cybercriminals, and PSD2 and Open Banking are set to offer hackers even more opportunities to steal sensitive personal and financial information," said Ed Cabrera, chief cybersecurity officer for Trend Micro. "Our concern is that the industry may not be fully prepared to deal with this greatly expanded attack surface. That's why we wanted to understand the risks before they occur, so we can help FinTechs and traditional lenders protect their assets first."

The report highlights several possible attack scenarios under the new regulatory regime:

- **Attacks on APIs:** Public APIs are at the heart of Open Banking, allowing approved third parties to access users' banking data to provide innovative new financial services. Implementation flaws in these APIs will allow attackers to exploit back-end servers to steal data.
- **Attacks on FinTech companies:** Users will be forced into a new trust relationship with providers that may have fewer resources than their banks and no track record on data protection. In a quick survey of Open Banking FinTechs, Trend Micro found them to have an average of 20 employees and no dedicated security professional. This makes them ideal targets for attackers and raises concerns over security gaps in their mobile apps, APIs, data sharing techniques and security modules that could be incorrectly implemented.
- **Attacks on the apps or mobile platforms:** Most Open Banking services will be deployed as mobile apps, making these a prime target for attackers. Finding the username, password, or encryption keys within the app would allow a criminal to retrieve banking data and pose as the user. Even if the apps don't have permission to make payments, they could contain transaction data, allowing an attacker to build a highly accurate profile of their victims.
- **Attacks against the user:** Because new Open Banking apps will become the primary means for users to access financial data and services, phishing attacks could reap major rewards for attackers.

To prepare for the changing landscape, Trend Micro details how financial institutions can improve their cyber resilience. These include ensuring sensitive information is never contained in URL paths, prioritizing secure protocols, and eliminating risky practices.

Meanwhile, Open Banking app developers and owners must adopt a secure-by-design approach, including regular software audits.

To find out more about the cyberrisks associated with new Open Banking rules, read our report, *Ready or Not for PSD2: The Risks of Open Banking,* here: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.
