# The Attack Surface of the Japanese Financial Services Industry

Japan is the third largest economy in the world, a distinction that makes it a natural target for cyber attackers. As a global hub for many industries including automotive, telecommunications & media, and manufacturing, Japan's attack landscape far exceeds just companies and organizations within the geographic boundaries of Japan.

The Japanese financial services industry is a major player on the world stage and one of the most complex and robust financial markets on the globe. It is a lucrative target for cyberattackers. In our latest report we take a look at the entire Japanese attack landscape and analyze the financial services industry specifically. Below are a few of the key trends and findings our researchers uncovered.

## Compromised Customer Data:

Financial Services companies are prime targets for attacks on credentials as having access to customer accounts is a direct financial risk to millions of potential victims. Phishing was the most common way attackers compromised financial institution's customers representing 31% of all attacks in the financial services sector we studied from 2021. Many of the attacks focused on English-language character strings indicating one hypothesis of the report that attackers prefer to attack subsidiaries that work in languages more commonly spoken globally than Japanese tends to be.

Our report uses threat intelligence on state-sponsored threat actors. One Chinese-based attack made the PII of more than 48,000 Japanese bank customers available for sale on criminal forums. These attacks often take the form of online banking credential and/or retail payment card information compromises. Third-party payment processors are also a potential source of bulk payment car data. In some cases, the banks themselves were targeted in order to obtain and sell large tranches of customer data.

## Compromised Employee Data:

While most attacks on Japanese financial institutions centered on obtaining the PII of customers and accessing their accounts, it was not uncommon for attackers to also target finserv organization employees. For instance, in November 2020, an attacker offered to sell the PII of more than 684,000 Japanese and Australian bank employees. That PII included credential pairs, national ID numbers, street addresses, phone numbers, email addresses, and other important identifiable information.

## Cryptocurrency Exchanges:

Japanese cryptocurrency exchanges have proven to be a lucrative target for cyberattackers with one of the most well-known breaches in history having come from the Tokyo-based Mt. Gox in 2014. Over the last few years, other exchanges have been victims of attacks, some of which began with vulnerabilities stemming from their overseas subsidiaries. In the example of Liquid, more than $97 million USD was stolen through the compromise of a Singaporean subsidiary's use of multiparty computation wallets that were less secure.

These are just a few of the impacts attackers have had on the Japanese financial services industry in just the last few years. For more on this sector and several others, read the report.