日本国内の金融業界における サイバー攻撃対象領域について

世界第3位の経済大国である日本は、それゆえ、サイバー犯罪の標的になりがちであるとも言えます。自動車、通信・メディア、製造業など、さまざまな産業のグローバル的中心地である日本を取り巻くサイバー攻撃は、日本国内の企業や組織にとどまらず、国外へと広がっています。

世界的に最も複雑で堅牢な金融市場を擁する日本の金融サービス産業は、国際的な金融市場を率いる存在であるため、サイバー攻撃者にとって格好の標的となっています。Rapid7のレポートでは、日本を取り巻くサイバー攻撃の全体像を概観しています。本書では、特に金融サービス業界を中心に分析した結果、Rapid7の研究者が明らかにした主要な傾向と調査結果をいくつかご紹介します。

顧客データの侵害

金融機関の場合、顧客口座への不正なアクセスが発生した際の影響が数百万件に及び、経済的な打撃につながるリスクがあります。そのため、認証情報目当ての攻撃の対象となりやすい傾向があります。金融機関の顧客を標的とする最も一般的な手口はフィッシングで、調査対象となった2021年以降の金融業界におけるの攻撃の31%を占めています。こうした攻撃では英語が使われているケースが多く、レポートでは、攻撃者が、日本語を使う日本国内企業を避け、英語使う海外子会社を攻撃の標的していると考えられています。

Rapid7のレポートでは、国家支援型脅威アクターに関する脅威インテリジェンスについても触れています。中国を拠点とするある攻撃の結果、48,000件を超える日本国内の銀行の顧客情報（PII）が犯罪フォーラムで販売されることになりました。こうした攻撃の多くは、オンラインバンキングの認証情報やクレジットカード情報を標的とした侵害です。一度に大量のカードデータが入手できる、サードパーティの支払処理業者が狙われることもあります。場合によっては、銀行自体を標的とし、販売を目的として大量の顧客データを窃取することもあります。

従業員データの侵害

日本国内の金融機関に対する攻撃の多くは顧客の個人情報（PII）の取得と口座へのアクセスを狙ったものですが、攻撃者が金融企業の従業員を標的にすることもあります。例えば、2020年11月には、ある攻撃者が日本とオーストラリアの684,000人以上の銀行員のPIIを売りに出しています。このPIIには、IDとパスワード、日本国内ではマイナンバーに相当する国民識別番号、住所、電話番号、メールアドレス、などの重要な個人情報が含まれていました。

暗号通貨取引所

サイバー攻撃者は、日本の暗号通貨取引所を好んで攻撃することがわかっています。2014年の東京を拠点とするMt. Goxに対する侵害は、歴史上最も有名なインシデントの1つとなりました。過去数年間に他の取引所も攻撃を受けており、その一部は海外子会社の脆弱性が発端となっています。Liquidの例では、シンガポールの子会社が安全性の低いマルチパーティ計算ウォレットを使用したことで、9,700万米ドル相当以上の暗号資産が盗まれました。

ここでは、日本国内の金融業界に対する攻撃の影響のごく一部をご紹介しました。同分野を始め、他のいくつかの分野に関する詳細な分析については、レポートをご覧ください。