15

金融トレンド・コラム

サイバー攻撃の対象は、提供者から利用者へ

金融システムとインターネットの10年

1990年代、インターネットの爆発的普及に伴い、オープンなネットワークを利用したビジネス拡大が起こった。この環境変化を受けて、それまで基幹システムや専用回線を中心としたクローズドなネットワーク中心にビジネスを展開していた金融機関もインターネットバンキングをはじめとするオープンなシステムの需要に直面し、情報セキュリティ技術を正しく理解して駆使する必要性が生じた。それから十数年が経過し、情報セキュリティ対策に関しては目覚しい高度化が行われ、金融機関のシステムは先進的堅牢性を実現しようとしてきた。しかしながらセキュリティリスクがゼロになる日は来ていない。

脅威の変遷

攻略がより困難になっていく金融機関のシステムを前に、攻撃者は利用者環境に標的を移していった。犯罪組織を中心とした攻撃者はフィッシングサイトやマルウェアを利用した無作為攻撃の成功体験を重ね、得られた情報を現金化する洗練された闇市場を形成、今や攻撃がビジネス化するに至っている。そこでは具体的なインターネットバンキングシステムの実装情報も取り扱われており、攻撃コードを標的システム毎にカスタマイズすることで、より巧妙に利用者を欺くようになった。用いられたのは、閲覧している画面を利用者の端末上で改竄したり、送受信情報を窃取したりするマン・イン・ザ・ブラウザ攻撃であり、その機能を搭載したマルウェアである。この攻撃はこれまでの対策の盲点を突くように設計されており、オンラインでの利用者からの取引トランザクションは汚染された可能性を念頭におかざるを得なくなった。

図表　金融システムとインターネットに関連した情報セキュリティトピック

日付	内容
1997.5	インターネットバンキング開始
2000.4	全銀協　インターネットバンキングにおける留意事項について　公表
2004.11	VISAを騙るフィッシングメール発生
2005	カード、ATM等金融情報システム関連の事故・犯罪事例頻発
2005.1	全銀協　偽造キャッシュカード対策に関して申し合わせ
2005.10	FFIEC　Authentication in an Internet Banking Environment 刊行
2006.3	FISC　金融機関等コンピュータシステムの安全対策基準 第7版　刊行
2006.3	金融庁　情報セキュリティに関する検討会　の設置
2006.7	米国Citibankに対するフィッシング詐欺が発生
2006.12	金融庁　ネットバンキングへの監視強化発表
2006	インターネットバンキング不正取引被害額が1億円を突破
2007.2	全銀協　事務局となりつつCEPTOAR設置(情報共有・分析機能)
2007.3	犯罪収益移転防止法成立
2009	Gumblar攻撃（Web改竄）が頻発
2010.1	SCNBにSQLインジェクション攻撃発生　8300人分の認証情報漏洩
2010.12	フランス財務省に150通の標的型メール攻撃
2011.6	53金融機関のインターネットバンキングの認証情報詐取発生
2011.10	乱数表を取得しようとするフィッシングメールが発生
2012.1	全銀協　インターネットバンキングのセキュリティ強化策について申し合わせ
2012.6	Operation High Roller攻撃が発生
2012.7	ENISA声明発表「全端末がマルウェアに感染している仮定を」

（出所）FISC　平成25年版　金融情報システム白書から一部引用

近年の動向と今後

近年では海外を中心に、マルウェアを利用した、金融業界のシステムに対するかなり大規模な攻撃が観測されており、そこでは利用者を欺きリアルタイムに金銭を不正取得する悪夢のような先進的攻撃が展開されている(Operation High Roller等)。これまで海外での先進的攻撃が国内で発生する場合、半年から1年程度遅延する傾向があり、これから起こることに備えるためにも国内に限らず欧米の規制当局やガイドラインの動向にも注目してゆきたい。これからの10年、安全対策やリスク管理は、自由化や国際化による競争激化に勝つために、ますます重要な要素となるのではないだろうか。

（NRIセキュアテクノロジーズ　木内 雄章）