Financial crimes observer

A publication of PwC's Financial Crimes Unit

SWIFT不正送金から得られた教訓 ―1億米ドルの不正送金を防ぐために

2016年2月、バングラデシュ中央銀行は、SWIFT（国際銀行間金融通信協会）ネットワークへのアクセスに利用する認証情報を窃取され、1億100万米ドルにのぼる不正送金の被害を受けた[1]。史上最大規模の被害を生んだ今回のサイバー攻撃は、バングラデシュ中央銀行におけるサイバーセキュリティ対策と金融犯罪対策および内部不正対策の弱点を突いて行われたものである。この攻撃により、従来サイロ化され個別に実施されていた金融犯罪リスク管理を統合する必要性が示される結果となった。

今回のサイバー攻撃において、攻撃者はバングラデシュ中央銀行におけるセキュリティ対策の弱点を突いたマルウェアを開発し、既に導入されているセキュリティ対策やネットワークログ管理システムを迂回する仕掛けを作成した。さらに、バングラデシュ中央銀行の正規の認証情報を利用してSWIFTネットワークに不正にアクセス[2]し、中継口座を開設することにより金融犯罪検知システムをも回避した。さらに、バングラデシュ中央銀行が使用しているプリンターの機種を含め、非常に詳細な情報が利用されていたことから、本件に対する従業員の関与が疑われている。

なお、ベトナムやエクアドルの銀行においても同様のサイバー攻撃が発生していることから、この攻撃はバングラデシュ中央銀行のみならず、複数の銀行を標的とした広範なキャンペーンの一部であったと考えられている。このことを踏まえ、金融機関においては、同様のサイバー攻撃が自社で発生することを想定し十分なセキュリティ対策を打つこと、また送金システムを標的としたサイバー攻撃に対し、これまで以上に注力して対応することが求められる。そのために、金融機関はサイバーセキュリティ対策と金融犯罪対策および内部不正対策の統合またはシームレスな連携に焦点を当てる必要がある。このことにより、脅威の全体像をより明確に捉えることが可能となり、不審なトランザクションの検知率の向上および調査の効率化が図られる。

さらに金融機関においては、同様のサイバー攻撃を十分に防御・検知できるよう、既存のサイバーセキュリティ対策、金融犯罪対策、内部不正対策を改善することが求められる。そのために、まず自社が同様のサイバー攻撃に十分に対応可能か判断するために送金システムの監視プログラムを追加し、さらに予防策、検知策、対応策のレビューを実施すべきである。また、振る舞い検知ツールの活用や顧客審査の強化を通して金融犯罪対策も強化するとともに、送金システムへのアクセス権の配布を必要最低限にし、内部不正リスクを低減する必要がある。

本レポートはバングラデシュ中央銀行で発生したサイバー攻撃を分析し、今後金融機関に求められる対応に関するPwCの見解を述べたものである。

pwc

サイバー攻撃の背景

2016年2月4日、攻撃者は不正に入手した認証情報を用いてSWIFTネットワーク上で一連の送金指示を作成した。当初、攻撃者は35回にわたり総額9億5,100万米ドルもの不正な送金指示を作成していたが、そのうちニューヨーク連邦準備銀行により実際の送金処理が行われたのは5件のみであり、実被害額は1億100万米ドルであった[3]。それ以外の送金指示は、バングラデシュ中央銀行への確認が取れなかったためニューヨーク連邦準備銀行では送金が行われなかった。

不正に送金された1億100万米ドルのうち、8,100万米ドルはフィリピンのカジノで資金洗浄が行われた。残りの2,000万米ドルはスリランカの口座に送金されたが、スリランカの銀行側が不審な送金指示であると判断したため、全額回収されている。

攻撃者が不正に作成した送金指示の全てが成功したものではなかったが、今回のサイバー攻撃は史上最も成功した銀行強盗の一つであると言える。今回の手口は、以下に述べる複数の要因が組み合わされたことにより成功したものと考えられる。一点目はバングラデシュ中央銀行におけるサイバーセキュリティ対策、金融犯罪対策、内部不正対策の弱点を突いたこと、二点目は攻撃者が銀行の送金システムの仕組みを熟知していたこと、三点目は特定の企業を標的としたマルウェアが利用されたこと(そのため今回は一般的なマルウェア対策プログラムでは検知することができなかった)、そして四点目は送金システムだけではなく、インシデントの検知プログラムや対応プログラムに対しても不正アクセスが行われていたことである。これらの要素を組み合わせて行われた今回のサイバー攻撃のように、個別システムを標的とした従来のサイバー攻撃の代わりに、ビジネスプロセス全体を標的としたサイバー攻撃が本格化するとみられている。

今回のサイバー攻撃に関するより詳細な情報は以下のとおりである。

- マルウェアはバングラデシュ中央銀行向けにカスタマイズされたものであり、同行で実際に利用されているプリンターの機種など、バングラデシュ中央銀行に関する詳細な情報をもとに作成されたものであったことから、従業員の関与または大規模な偵察があったものとみられている
- マルウェアにはバングラデシュ中央銀行が利用していたソフトウエアやシステムによる検知を回避する機能が備えられていたことから、攻撃者はSWIFTネットワークやデータベースの構造を含め、送金システムのソフトウエアや仕組みに関する詳細な知識を持っていたと考えられる
- 攻撃者は、サイバー攻撃の検知を目的として設計されたネットワークログ管理システムを不正に操作していた
- 攻撃者は、同行のプリンターをも不正に操作し、不正なトランザクションを隠ぺいするために確認用メッセージを偽造していた
- 資金の送金・着金には、休眠口座が利用されていた

金融機関に求められる対応

金融機関においては、不正送金被害に遭う前に、このようなサイバー攻撃に対する十分な対策を取る必要がある。まずは、バングラデシュ中央銀行で発生した不正送金と同様の被害を既に受けているのか、または標的となっている状態であるかを明らかにするために、従来のセキュリティログ分析よりもさらに詳細な調査を実施することが望ましい。

あわせて、バングラデシュ中央銀行で発生したサイバー攻撃の手口を模した新たな攻撃に備え、対策を実施する必要がある。そのためには、個別に導入されている既存のサイバーセキュリティ対策のみに依存するのではなく、サイバーセキュリティ対策、金融犯罪対策、内部不正対策を一元的に管理することが望ましい。さらに、サイバーセキュリティ対策、金融犯罪対策、内部不正対策を強化するために、過去のサイバー攻撃から学んだ教訓を活用するべきである。

高度化する金融犯罪に対応するためには、以下のステップに沿った対応の実施が推奨される。

金融犯罪領域の統合

- 従来個別に管理されていた金融犯罪に関する情報を管理用データベースに移し、一元的に管理する。このデータの活用により、不審なトランザクションを識別することが可能となる。ただし、取引量の多い金融機関においては、大量のトランザクションデータから不審なトランザクションを識別するための分析用エンジンが必要となるものと考えられる[4]
- 金融犯罪に関する包括的なリスク評価を実施する
  - 金融犯罪の傾向、発生状況、類似犯罪の発生予測(バングラデシュ中央銀行に対するサイバー攻撃や送金システムを標的とした同様のサイバー攻撃を含む)に基づく評価および優先順位付け
  - 攻撃の重要度や発生可能性、コントロールされている資産の評価
  - 現状のセキュリティ対策状況に基づくリスク評価およびセキュリティ対策やプロセスの改善提案
- 一元化された金融犯罪管理システムを構築する。現在、多くの金融機関において、さまざまな金融犯罪の領域(例:サイバーセキュリティや金融犯罪)を管理するために複数のシステムが併用されている。このため、不正調査の担当者は異なる領域で発生したインシデントについて関連性があるか判断できずにいる。今後はインシデントを統合的に管理し、サイバー攻撃への対応の迅速化や調査の優先順位付けの改善、調査作業の効率化を図ることが期待される[5]
- インシデントの報告先やコミュニケーション計画の定義など、調査に関する一元的な管理プロセスを確立する

サイバーセキュリティ対策

- 同様のサイバー攻撃に対応するうえで必要なサイバーセキュリティ対策が自行において実施されているかを検証するために、防御策、検知策、対応策の詳細なレビューを実施する[6]
- 公開されているレポートや業界内の情報共有組織、SWIFT（国際銀行間通信協会）、脅威情報サービスから入手した情報を活用し、攻撃手法や攻撃に用いられる固有の識別子（例：ファイル名、ネットワーク通信構造）を特定する。また、入手した情報をもとに、自社の重要システムにこれらの識別子が存在するか、詳細な調査を行う
- SWIFTデータベースと接続されるプロセスを監視し、新規プロセスの生成を検知した際にアラートを上げる仕組みを実装する
- SWIFTとの接続のあるシステムやその他の送金システムなど、重要システムから外部に送信される通信を監視する
- SWIFT決済用ソフトウエアを最新化する（例：SWIFT Alliance Access、Alliance Entry）

金融犯罪対策

- 複数回のログイン失敗のような不審なトランザクションの検知や分析を実施するために、振る舞い検知機能を実装する[7]
- 休眠口座において、海外への多額の資金移動や国内のバッチ処理（特に、カジノのようなリスクの高い宛先への送金処理）といった大量のトランザクションが突然発生した場合、KYC（Know your customer：顧客確認のプログラム）やマネーロンダリング防止に関するポリシーを遡及的に適用する。また、リスクの高い顧客には、標準よりも強固な検証機能や取引の保留機能を強制的に実装する[8]
- 帯域外で行われる確認作業（例：書面やメール、音声による確認）についてレビューを行う、またソーシャルエンジニアリングを含め、送金業務において不正がどのように発生しうるか理解する[9]
- SWIFTや他の送金プラットフォームで発生しうる不正を類型化し、十分な防御策および検知策が実装されているか評価する。特に、以下の観点が含まれることが望ましい
  - 認証ルール
  - 取引の承認ルール
  - 不正取引監視
- 不正リスク評価を通して識別された不審な活動を精査し監視する。特に銀行においては、取引の承認プロセスを重点的に監視することが推奨される[10]

内部不正対策

- SWIFTや他の送金システムへのアクセス権を持つ人（例：従業員、契約社員、プログラマー、外部業者）を識別する
- 送金システムへのアクセス権には最小権限の原則を適用する。また、最小権限の原則に従いユーザーのニーズや業務上の必要性を評価し、アクセス権を付与する対象者を制限する
- 送金手続きに関するポリシーや手順において、送金処理の担当者と承認者に関する要求事項（例：送金処理の作業者と承認者は別の人物とする）を定義する。また、送金処理の承認者は内部共謀の抑制に十分な権力を持つポジションとするよう定める
- アクセス権の不正利用、または所定の権限を超過したユーザーの活動を監視する。認証情報や送金システムへのアクセスの中から不正を検知するための分析プログラム（例：過剰なログインや業務時間外のアクセス）を導入し、アラートを調査する
- 送金システムへのアクセスを行う全ての従業員に対し、バックグラウンドチェックを実施する
- 内部通報制度を従業員や管理者向けのポリシーに導入する。エスカレーションや内部通報に関するポリシーや手順の整備だけではなく、脅威の検知や不審な振る舞いの報告に関する教育を実施する

注釈

1. SWIFTは、資金移動を目的として金融機関が利用するネットワークである。海外送金の多くはSWIFTネットワークを経由して行われている
2. 攻撃者がどのようにバングラデシュ中央銀行の認証情報を窃取したかについては、未だ解明されていない。攻撃者が銀行口座や決済システムの認証情報の窃取に用いたと思われるさまざまな手法に対するPwCの考察は、PwC “Financial crimes observer, Fraud：Email compromise on the rise（2016年2月）”を参照
3. ニューヨーク連邦準備銀行は、およそ250の海外の中央銀行（バングラデシュ中央銀行を含む）の口座を管理しており、各銀行に対する決済サービスを提供している
4. データアナリティクスに関する詳細情報は、PwC “Financial crimes observer, Bank fraud：Old defenses won’t stop new threats（2016年4月）”を参照
5. 金融犯罪管理システムに関する詳細情報は、注釈4.と同じレポートを参照
6. サイバーセキュリティにおける防御策、検知策、対応策に関する詳細情報は、PwC “A closer look, Cyber：Think risk, not IT（2015年4月）”を参照
7. 振る舞い検知に関する詳細情報は、注釈4.と同じレポートを参照
8. KYC（Know your customer：顧客確認のプログラム）や顧客審査の詳細情報は、PwC “Financial crimes observer, AML：Who is your customer? FinCEN wants you to know（2016年5月）”を参照
9. 認証に関するセキュリティ対策の回避に用いられるソーシャルエンジニアリングに関する詳細情報は、注釈2.と同じレポートを参照
10. 不正リスク評価に関する詳細情報は、注釈4.と同じレポートを参照

お問い合わせ先

PwCコンサルティング合同会社

〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
TEL：03-6250-1200（代表）

山本 直樹（Naoki Yamamoto）
サイバーセキュリティ リーダー
080-2105-3073
naoki.n.yamamoto@pwc.com

サイモン・ギーリー（Simon Gealy）
フィナンシャルサービス リーダー
080-3549-9530
simon.s.gealy@pwc.com

ショーン・キング（Sean King）
サイバーセキュリティ パートナー
080-4366-6596
sean.c.king@pwc.com

マイケル・バクストン（Michael Buxton）
リスクコンサルティング リーダー
090-9138-7630
michael.buxton@pwc.com

ジョセフ・ダブズ（Joe Dubbs）
サイバーセキュリティ ディレクター
080-4061-7440
joseph.dubbs@pwc.com

www.pwc.com/jp

本報告書は、PwCメンバーファームが2016年6月に発行した『SWIFT action: Preventing the next $100 million bank robbery』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 www.pwc.com/us/en/financial-services/financial-crimes/publications/swift-bangladesh-robbery-2016.html
日本語版発刊月： 2016年10月　　管理番号： I201609-5