報道関係者各位
プレスリリース

2014 年 6 月 5 日
株式会社 FFRI

FFRI、国内主要金融機関 9 社の利用者を狙うオンライン不正送金手口を検証
～MITB 攻撃対策製品「FFRI Limosa」の有効性を確認～

2014 年 6 月 4 日発表　弊社プレスリリース「FFRI、国内主要金融機関 8 社の利用者を狙うオンライン不正送金手口を検証　～MITB 攻撃対策製品「FFRI Limosa」の有効性を確認～」におきまして、記載内容に誤りがございました。下記の通り訂正させていただきます。

【訂正前】
FFRI、国内主要金融機関 8 社の利用者を狙うオンライン不正送金手口を検証
～MITB 攻撃対策製品「FFRI Limosa」の有効性を確認～

【訂正後】
FFRI、国内主要金融機関 9 社の利用者を狙うオンライン不正送金手口を検証
～MITB 攻撃対策製品「FFRI Limosa」の有効性を確認～

【訂正前】
今回、FFRI が入手した MITB 攻撃マルウェアを解析した結果、国内の主要銀行 4 行と信販会社 4 社の利用者を標的としていることが判明したため、実際に標的とされている銀行のアカウントで検証し、「FFRI Limosa」で防御できることを確認しました。

【訂正後】
今回、FFRI が入手した MITB 攻撃マルウェアを解析した結果、国内の主要銀行 4 行と信販会社 5 社の利用者を標的としていることが判明したため、実際に標的とされている銀行のアカウントで検証し、「FFRI Limosa」で防御できることを確認しました。

以下、リリース内容となります。

株式会社 FFRI（本社：東京都渋谷区、代表取締役社長：鵜飼 裕司、以下 FFRI）は、ワンタイムパスワードによる認証を突破し、ネットバンキング利用者の口座から不正送金を行う MITB（Man in the Browser）攻撃※1 マルウェアを入手し、解析・検証を実施した結果、FFRI の MITB 攻撃対策製品「FFRI Limosa」による防御が有効であることを確認しましたのでお知らせします。

MITB 攻撃の進化 ～パスワードの搾取から不正送金の自動実行へ～

2012 年秋以降、日本で発生していた MITB 攻撃は、MITB マルウェアが搾取した認証情報によるなりすましが不正送金に繋がっていました。従来の攻撃手法の場合、有効期間の短いワンタイムパスワードの利用により、認証情報の搾取から不正送金の実行までの時間的制約が被害を抑止していた面もあったと思われますが、2014 年春以降に発生している被害では、MITB マルウェアがワンタイムパスワードを搾取すると同時に、不正送金処理まで自動実行するタイプに進化しており、被害金額も既に昨年度のペースを大きく上回るスピードで拡大していることが報道されています。

MITB 攻撃マルウェアの仕組みと、「FFRI Limosa」による防御技術

MITB 攻撃は、ネットバンキング利用者の PC 端末に感染※2 したマルウェアが Web ブラウザに侵入することが必要となります。Web ブラウザへの侵入後は、利用者が正規の手順で認証を済ませた後、ブラウザの処理を横取りすることが可能なため、ワンタイムパスワードなどによる認証の強化は十分な対策とは言えません。実際に、2014 年春以降の MITB 攻撃ではワンタイムパスワードを利用している利用者においても被害が発生しています。

今回、FFRI が入手した MITB 攻撃マルウェアを解析した結果、国内の主要銀行 4 行と信販会社 5 社の利用者を標的としていることが判明したため、実際に標的とされている銀行のアカウントで検証し、「FFRI Limosa」で防御できることを確認しました。具体的には、「FFRI Limosa」によって保護された Web ブラウザの利用時に MITB 攻撃マルウェアによる Web ブラウザへの侵入を阻止し、「FFRI Limosa」が適用されていない状態で検証した際に表示されていたプログレスバーやワンタイムパスワードを要求する偽画面が表示されないことを確認しています。

「FFRI Limosa」は、Web ブラウザの堅牢化により、MITB 攻撃マルウェアが Web ブラウザに侵入することを防ぎます。ウイルス対策ソフトと違って個々のマルウェアを識別・対応する必要がなく、未知の MITB 攻撃マルウェアに対しても効果を発揮できるのが特徴です。

【製品情報】

FFRI Limosa

http://www.ffri.jp/products/limosa/index.htm

「FFRI Limosa」関連ページ

「ネットバンキングユーザーを狙った MITB 攻撃の脅威と対策製品の比較検証」

http://www.ffri.jp/special/mitb_1.htm

■FFRI について

当社は 2007 年、日本において世界トップレベルのセキュリティ・リサーチ・チームを作り、コンピューター社会の健全な運営に寄与すべく設立されました。現在では日々進化しているサイバー攻撃技術を独自の視点で分析し、日本国内で対策技術の研究開発に取り組んでいます。研究内容は国際的なセキュリティカンファレンスで継続的に発表し、海外でも高い評価を受けておりますが、これらの研究から得られた知見やノウハウを製品やサービスとしてお客様にご提供しています。主力製品となる、「FFR yarai」はミック経済研究所※3 および富士キメラ総研調べ※4 によるエンドポイント型標的型攻撃対策分野における出荷金額において No.1 を獲得しております。

※1 インターネットバンキング利用者の端末に侵入したマルウェアが、Web ブラウザを不正に操作することで、認証情報の奪取や不正送金を行うサイバー攻撃の一つ。

※2 正規の Web サイトの改ざんにより、Web サイトを閲覧しただけで日本の金融機関の利用者を標的とした MITB 攻撃マルウェアに感染するドライブバイダウンロードによる攻撃が複数の Web サイトで確認されていることが各種メディアから報道されています。

※3 出典：ミック経済研究所「情報セキュリティソリューション市場の現状と将来展望 2013【外部攻撃防御型ソリューション編】」

※4 出典：富士キメラ総研「2013 ネットワークセキュリティビジネス調査総覧【上巻 市場編】」

本リリースに関するお問い合わせ先
写真・資料等がご入用の場合もお問い合わせください。
株式会社 FFRI
経営企画部 PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp URL：http://www.ffri.jp