報道関係者各位
プレスリリース

2015 年 10 月 14 日
株式会社 FFRI

FFR yarai がバンキングマルウェア「SHIFU」を検知・防御
～パターンファイルに依存せず、最新のマルウェア動向研究の知見を活かして～

サイバーセキュリティ領域において国内で独自の研究開発活動を展開している株式会社 FFRI（本社：東京都渋谷区、代表取締役社長：鵜飼裕司、以下 FFRI）は、2015 年 10 月 14 日、標的型攻撃対策ソフトウェア「FFR yarai」および個人・SOHO 向けセキュリティソフト「FFRI プロアクティブ セキュリティ（製品愛称：Mr.F）」がバンキングマルウェア「SHIFU」をリアルタイムに検知・防御が可能であったことをご報告いたします。

バンキングマルウェア「SHIFU」 vs. FFR yarai

2015 年 10 月 8 日、“特定の組織からの注文連絡”や“複合機からの自動送信”を装った Word 文書ファイルが添付された不審なメールに関する相談が相次ぎ、IPA からの注意喚起がなされています。IPA によると、添付の Word 文書ファイルはマクロ※1 を実行してマルウェアをダウンロードする機能を有しており、この Word 文書ファイルを開いた場合にはマルウェア感染の可能性があることがわかりました。

※1 ソフトウェア内で使用される複数のコマンドをまとめて実行する機能。マクロを実行してマルウェアに感染させる攻撃手法は 2014 年後半から増加傾向にあり、バンキングマルウェア「DRIDEX」（2015 年 3 月）も同様の攻撃手法を使っています。

身に覚えのない不審なメールを受信した場合は、添付ファイルを開いたり実行したりしないようご注意ください。

これらの偽装メールに添付された Word ファイルに含まれる不正マクロは、当初からマクロが有効になっている場合、もしくはマクロを有効化してしまった場合に実行されます。近年は Microsoft Office のマクロ機能がデフォルトで無効化されていますが、業務の必要性から有効にしているユーザーも存在していると思われます。ユーザーの皆様には今一度デフォルト設定の見直しを強く推奨いたします。

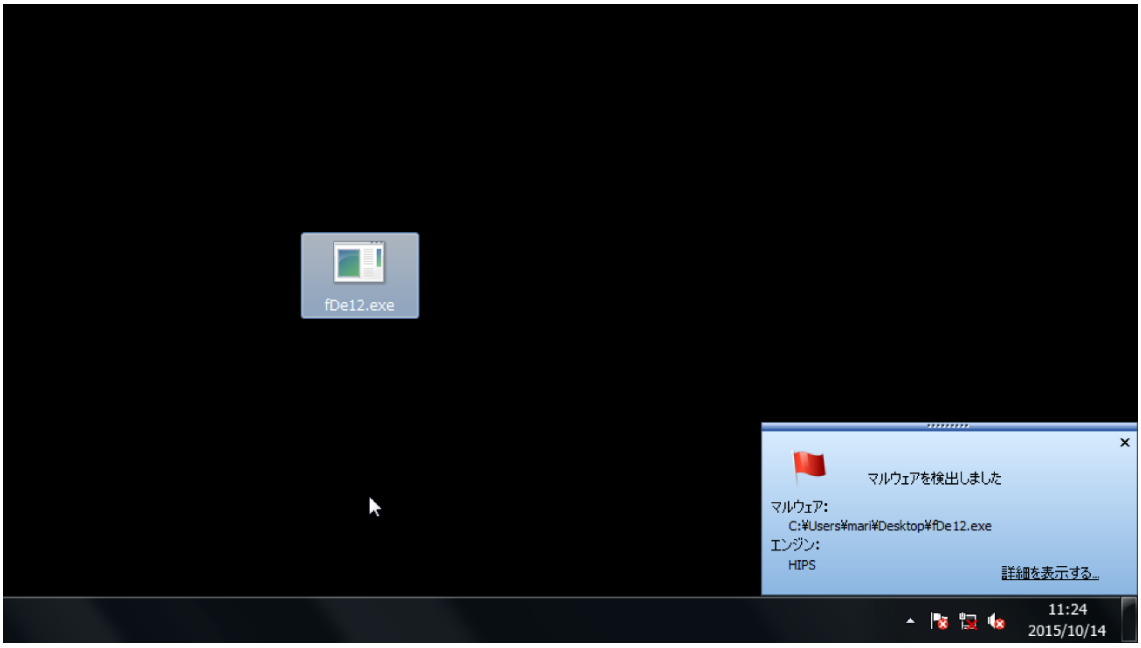
このたび悪用された不正マクロは、「SHIFU」と呼ばれるバンキングマルウェアをダウンロードするものです。
「SHIFU」は今年 4 月ごろから広がり始め、日本の銀行 14 行を攻撃対象としていたことが報道されています。

FFRI では今回問題となっている Word 文書ファイルを入手し、検証を行った結果、下記の 2 製品で「SHIFU」を検知・防御できることを確認いたしました。

■検証環境
Windows 7 Pro 64bit × FFR yarai 2.6.1294（2015 年 6 月 4 日リリース）
Windows 7 Pro 64bit × FFRI プロアクティブ セキュリティ 1.1.345（2015 年 7 月 21 日リリース）

■検証した検体のハッシュ値（SHA-256）
7c2f867cbca04c854ce43085e24c7f2e9b934a2165928d6e528bfb97f4840bb1

検証結果は、画面キャプチャのとおり、FFR yarai の 5 つのヒューリスティックエンジンの中の動的解析を担う HIPS エンジンがマルウェアを検知してシステムを保護しています。



【FFR yarai 検知画面】

今回の検証で使用した FFR yarai 2.6.1294 は、2015 年 6 月 4 日にリリースしており、本製品をご利用いただいていた場合、今回同様の手法を用いた攻撃を未然に防ぐことができたといえます。

FFRI は、今後も独自の調査・分析を行い、脅威を先読みすることで真に価値のある対策を社会に提供できるよう日々精進していく所存です。

◎法人向け

【製品名称】

FFR yarai

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

【FFR yarai の防御実績】 これまでに防御した攻撃・マルウェア一覧

http://www.ffri.jp/products/yarai/defense_achievements.htm

◎個人・SOHO 向け

【製品名称】

FFRI プロアクティブ セキュリティ （製品愛称：Mr.F）

http://www.ffri.jp/online_shop/proactive/index.htm

■標的型攻撃対策ソフトウェア「FFR yarai」とは

FFR yarai シリーズは、従来のセキュリティ対策で用いられているシグニチャやパターンファイルなどに依存せず、標的型攻撃で利用される攻撃の特徴を 5 つのヒューリスティックエンジンにより、様々な角度から分析し、未知の脅威に対して高い精度で攻撃を検知・防御します。純国産の技術で開発した製品で、厳格なセキュリティ対策が求められる官公庁や重要インフラ企業、金融機関での採用実績が多数あります。

韓国の放送局や銀行などがシステムダウンした韓国サイバー攻撃（2013 年 3 月）、ソニー・ピクチャーズエンターテイメント社に対する一連のサイバー攻撃に関連するシステム破壊型マルウェア（2014 年 12 月）、Adobe Flash Player の脆弱性（2015 年 1 月）、ハードディスクのファームウエアの書き換えを行う HDD ファームウェア感染マルウェア（2015 年 2 月）、ネットバンキングユーザーを狙ったバンキングマルウェア（2015 年 3 月）、日本年金機構を狙ったマルウェア「Emdivi」（2015 年 6 月）等、これまでに防御した攻撃・マルウェアを防御実績として FFRI ホームページにて公開しています。

■株式会社 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、コンピュータ社会の健全な運営に寄与するために設立されました。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調べ※2 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。

※2　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 2015【外部攻撃防御型ソリューション編】」

本件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
経営管理本部　PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp