報道関係者各位
プレスリリース

2015 年 3 月 11 日
株式会社 FFRI

2014 年ネットバンキング不正送金被害額は約 29 億 1,000 万円！
FFR yarai がネットバンキング利用者を狙うバンキングマルウェア「DRIDEX」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 3 月 11 日、標的型攻撃対策ソフトウェア「FFR yarai」がネットバンキング利用者を狙うバンキングマルウェア「DRIDEX」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。

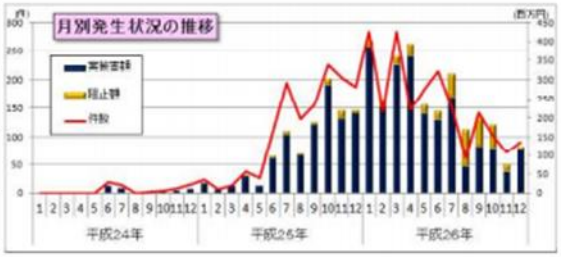
手口の悪質・巧妙化が進むネットバンキングキング不正送金、被害額は約 29 億 1,000 万円

2015 年 2 月 12 日、警察庁から「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」が発表されました。
これによると、2014 年のオンラインバンキングからの不正送金被害額が約 29 億 1,000 万円と 2013 年から倍増しており、不正送金処理を自動で行うマルウェアが利用される等、手口の悪質・巧妙化が進んでいることがわかります。

平成26年中のインターネットバンキングに係る
不正送金事犯の発生状況等について

1　平成26年中の発生状況
（1）発生件数及び被害額　　１，８７６件　約２９億１０００万円

期間	件数	被害額（実被害額）
H26	1,876件	約29億1000万円（約24億3600万円）
H25	1,315件	約14億 600万円（約13億3000万円）
H24	64件	約 4800万円（約 4800万円）



※　被害額　・・・犯人が送金処理を行ったすべての額
※　実被害額・・・「被害額」から金融機関が不正送金を阻止した額を差し引いた実質的な被害額

出典：警察庁「平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」
http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

ネットバンキング不正送金を行うバンキングマルウェア「DRIDEX」 vs.FFR yarai

FFRI では、ネットバンキング利用者の口座から不正送金を行うバンキングマルウェア「DRIDEX」を入手し、検証を行いました。このマルウェアはメールに XML ファイルを添付し、ファイル中に含まれるマクロを実行させることで感染活動を行うバンキングマルウェア (MITB※1 マルウェア)です。

※1 Man in the Browser の略。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。

動作は通例のバンキングマルウェアと同様ですが、感染経路に XML ファイルを使用しているという特徴があり、世界的な広がりを見せています。2015 年 1 月に Microsoft 社から Office のマクロ機能を悪用してマルウェアに感染させる手口が増えているとして注意喚起がありましたが、今回の XML ファイルも実行すると Word が立ち上がり、Office のマクロ機能を実行することで感染するものです。

FFRI では当該のマクロデータが含まれる XML 形式の Word ドキュメントを入手し、マクロ部分を抽出、難読化を解除後、暗号化されている文字列を復号し、解析したところ、この XML ファイルが「ダウンローダー」と呼ばれる感染後に別のマルウェアをダウンロードさせ、攻撃を行うものである可能性が高いことがわかりました。

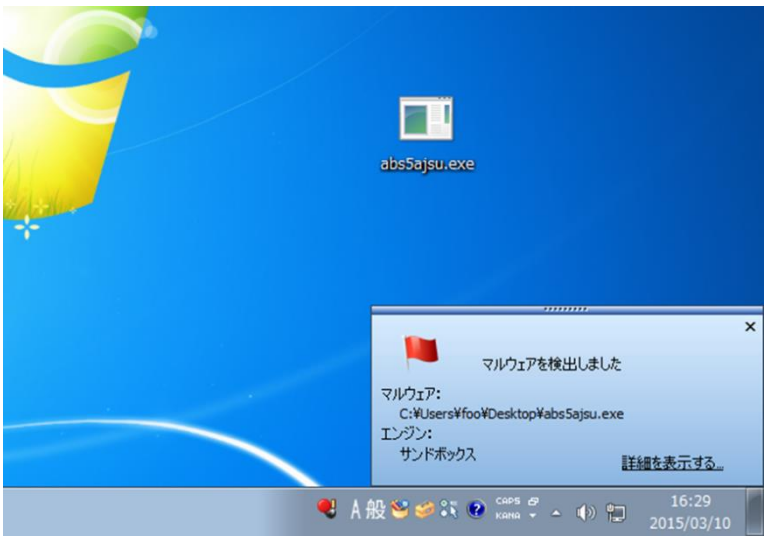
このマクロの解析結果からマルウェアを入手して検証を行った結果、FFRI の標的型攻撃対策ソフトウェア「FFR yarai」がこのマルウェアを Sandbox エンジンにより検知し、同様の攻撃を防御できることを確認しました。

■検証環境
Windows 7 x86 SP1
FFR yarai 2.5.1216.0（2014 年 12 月 10 日リリース）

■検証した検体
File: abs5ajsu.exe
SHA256:
34ba83169c0475b1731e267e8ca3bc20f5c1b618df4c05737a8c000d59266c3c

検証結果は、下記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 Sandbox エンジン※2 がマルウェアを検知してシステムを保護しています。

※2 仮想 CPU、仮想メモリ、仮想 Windows サブシステムなどで構成される仮想環境上でプログラムを実行させ、振る舞いを見てマルウェアらしさを判断する検知エンジンです。



今回の検証で使用した FFR yarai 2.5.1216.0 は、2014 年 12 月 10 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、今回のマルウェアを検知できていたといえます。

FFR yarai はパターンファイルを一切使用しておりませんが、FFRI のエンジニアが最新のマルウェアの動向を研究し、その知見を反映したプログレッシブ・ヒューリスティック技術を搭載しているため、マルウェアの構造や振る舞いを見て攻撃を検知・防御することが可能です。

■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）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。

【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

■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※3 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。

※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 2014【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
経営企画部　PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp