



**FFR yarai および FFRI プロアクティブ セキュリティが
不正送金マルウェア「URLZone」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 F F R I（本社：東京都渋谷区、代表取締役社長：鵜飼裕司、以下 FFRI）は、2016年2月10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）」が不正送金マルウェア「URLZone（別名：「Shiotob」「Bebloh）」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。

不正送金マルウェア「URLZone」 vs. FFR yarai

2015年12月中旬ごろから2016年1月下旬にかけて、不審なメールを介して国内のオンラインバンキングユーザーを狙った不正送金マルウェア「URLZone」の感染被害が報告されています。「URLZone」に感染するとオンラインバンキングや web やメールの認証情報を窃取されるおそれがあります。

「URLZone」を送り付ける不審なメールには、下記のような特徴が指摘されています。

- ・件名は英語または日本語
- ・本文には「返事待ってます」「お世話になっております」などの日本語の短文
- ・メールには文書ファイル（.doc）や画像ファイル（.jpg）などに偽造された「URLZone」を圧縮した zip ファイルが添付され、誤って開くと感染する
- ・「URLZone」には自身が実行されていることを隠蔽し、検知されにくくする機能を実装

FFRI では今回問題となっている「URLZone」の検体を2種類入手し、検証を行った結果、下記のとおり検知・防御できることを確認いたしました。

【検体 1 の検証結果】

■ 検証環境

Windows 7 × FFR yarai 2.6.1299 (2015 年 7 月リリース)

Windows 7 × FFR yarai 2.7.1410 (2015 年 7 月リリース)

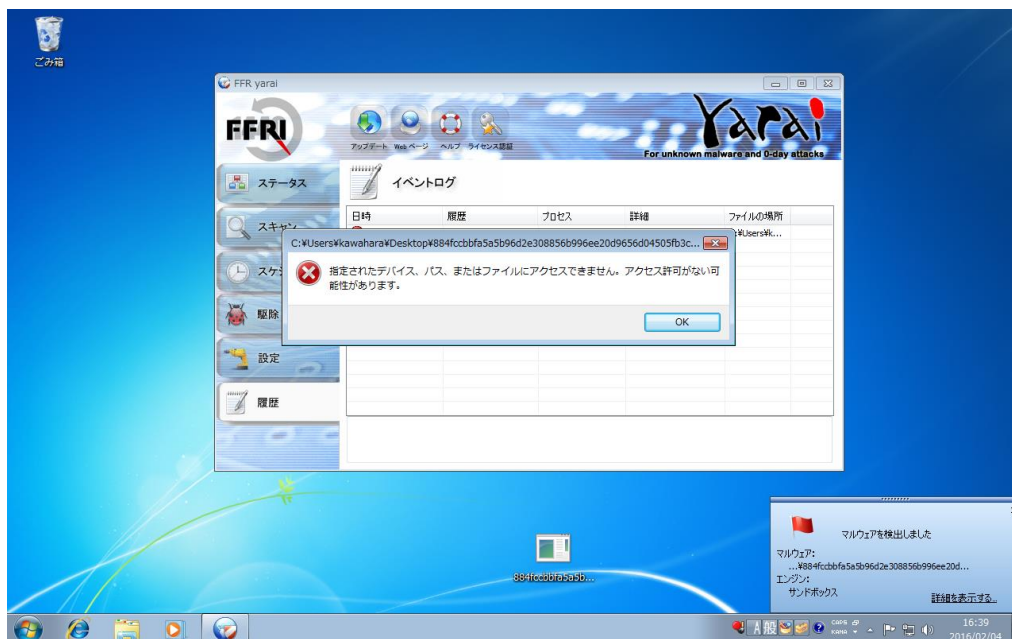
Windows 7 × FFRI プロアクティブ セキュリティ 1.0.227 (2015 年 7 月リリース)

Windows 7 × FFRI プロアクティブ セキュリティ 1.1.395.2 (2016 年 1 月リリース)

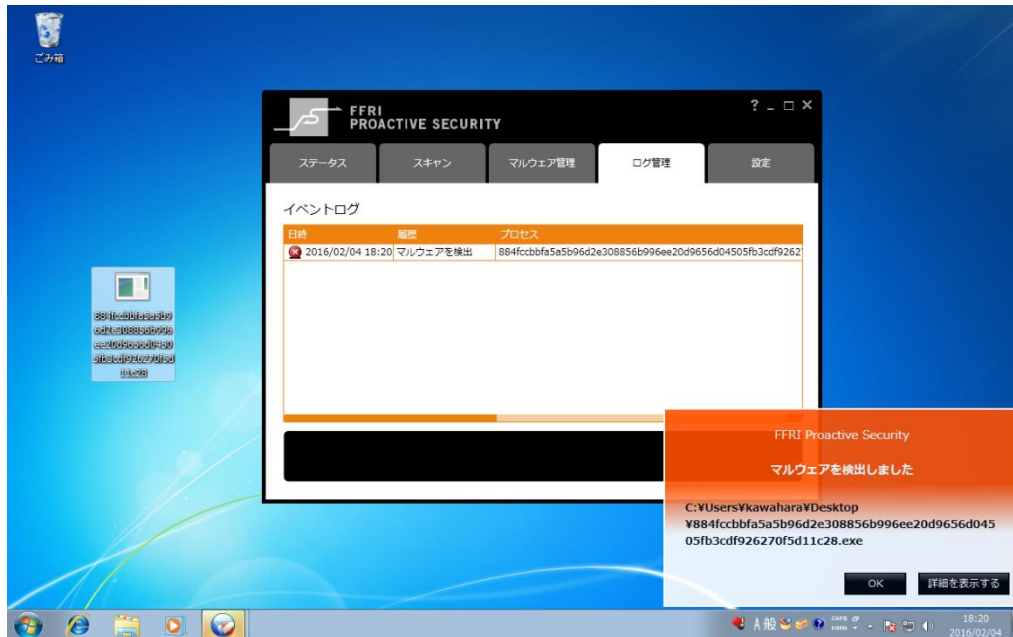
■ 検証した検体のハッシュ値

884fccbbfa5a5b96d2e308856b996ee20d9656d04505fb3cdf926270f5d11c28

検証結果は、画面キャプチャのとおり、FFR yarai および FFRI プロアクティブ セキュリティの 5 つのヒューリスティック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】



【FFRI プロアクティブ セキュリティ検知画面】

今回の検証で使用した FFR yarai 2.6.1299、FFRI プロアクティブ セキュリティ 1.0.227 はともに 2015 年 7 月にリリースしており、これ以降のバージョンの上記 2 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。

【検体 2 の検証結果】

■ 検証環境

Windows 7 × FFR yarai 2.7.1410 (2015 年 11 月リリース)

Windows 7 × FFRI プロアクティブ セキュリティ 1.1.395.2 (2016 年 1 月リリース)

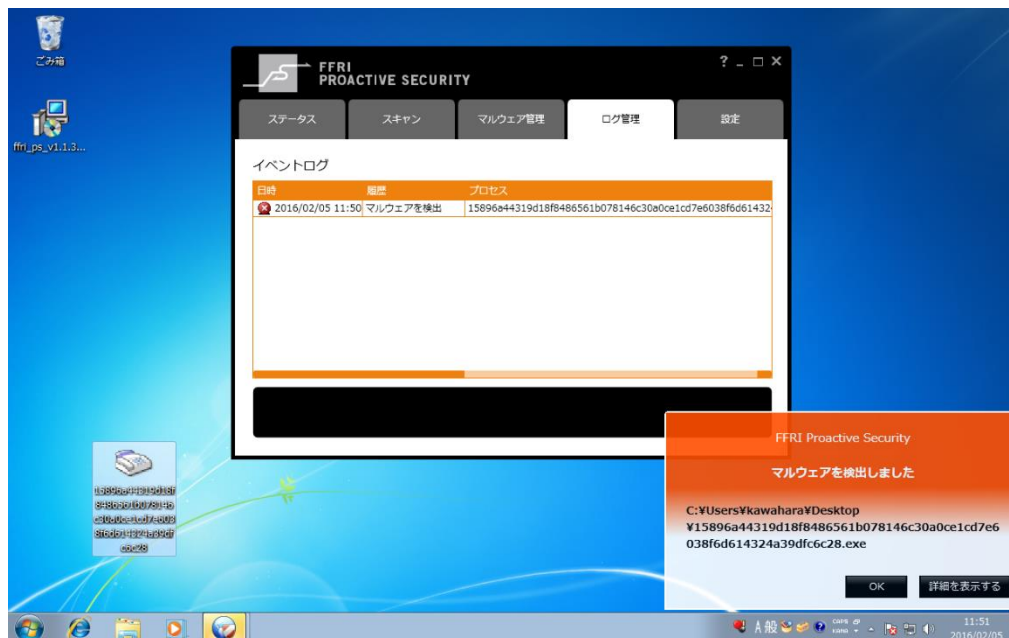
■ 検証した検体のハッシュ値

15896a44319d18f8486561b078146c30a0ce1cd7e6038f6d614324a39dfc6c28

検証結果は、画面キャプチャのとおり、FFR yarai および FFRI プロアクティブ セキュリティの 5 つのヒューリスティック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】



【FFRI プロアクティブ セキュリティ検知画面】

今回の検証で使用した FFR yarai 2.7.1410 は 2015 年 11 月、FFRI プロアクティブ セキュリティ 1.1.395.2 は 2016 年 1 月にリリースしており、これ以降のバージョンの上記 2 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ン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ェ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）、バンキングマルウェア「SHIFU」（2015 年 10 月）、ランサムウェア「TeslaCrypt (vvv ウイルス)」（2015 年 12 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 F F R I 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^{※1}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 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>

「F F R I」、「FFR yarai」、「FFRI プロアクティブ セキュリティ」、「Mr.F」は、株式会社 FFRI の登録商標です。

その他すべての社名、製品・サービス名は、各社の商標または登録商標です。

出典資料の引用等、調査会社の著作物を利用する場合は、出典元にお問い合わせください。