報道関係者各位
プレスリリース

2016年6月17日
株式会社ＦＦＲＩ

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「Gozi」をリアルタイムに検知・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、2016年6月17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、ネットバンキングユーザーを狙った不正送金マルウェア「Gozi」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「Gozi」 vs. FFR yarai

2016年5月末ごろから不正送金マルウェア「Gozi」（別名：「Ursnif」「Snifula」「Papras」）の感染被害が相次いで報道されています。感染の拡大について日本サイバー犯罪対策センター（JC3）から注意喚起※1が行われています。

同マルウェアは PC のキーボードから入力される情報を外部に送信する「キーロガー」の機能等を持っており、IDやパスワード等のネットバンキングのアカウント情報やクレジットカード情報を窃取し、感染するとネットバンキングから不正送金が行われたり、クレジットカードが不正利用されたりする恐れがあります。

また、感染経路としては下記のような例が報告されています。
・「請求書」「請負契約書」「支払確認」「年休申請」等を装ったメールに添付された偽装ファイルを開封
・改ざんされた web サイトを閲覧　等

※1　出典：インターネットバンキングマルウェア「Gozi」による被害に注意（JC3）
https://www.jc3.or.jp/topics/gozi.html

【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 2.7.1437 (2016 年 3 月リリース)

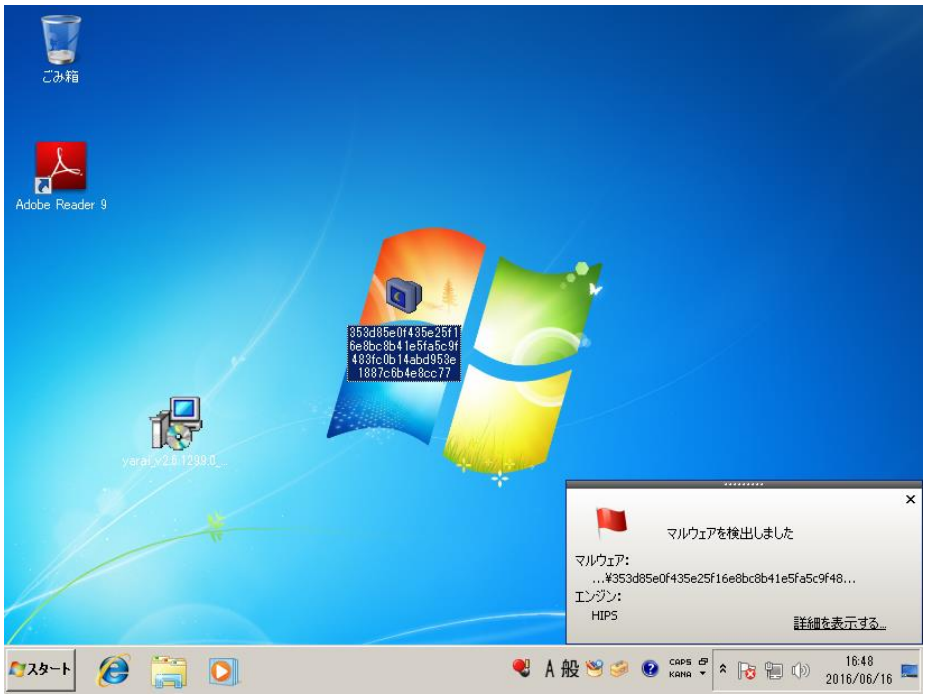
Windows 7 × FFRI プロアクティブ セキュリティ 1.0.227（2015 年 7 月リリース）

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）

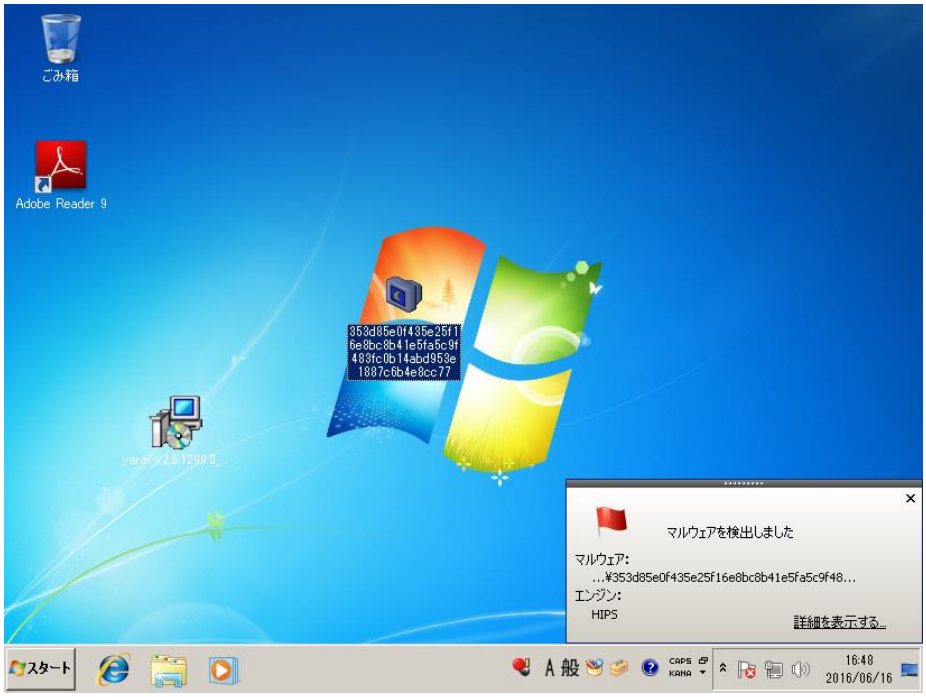
■検証した検体のハッシュ値

SHA256：353d85e0f435e25f16e8bc8b41e5fa5c9f483fc0b14abd953e1887c6b4e8cc77

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 2.6.1299 検知画面】



【FFRI プロアクティブ セキュリティ 1.0.227 検知画面】

【検体 2 の検証結果】

■検証環境

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

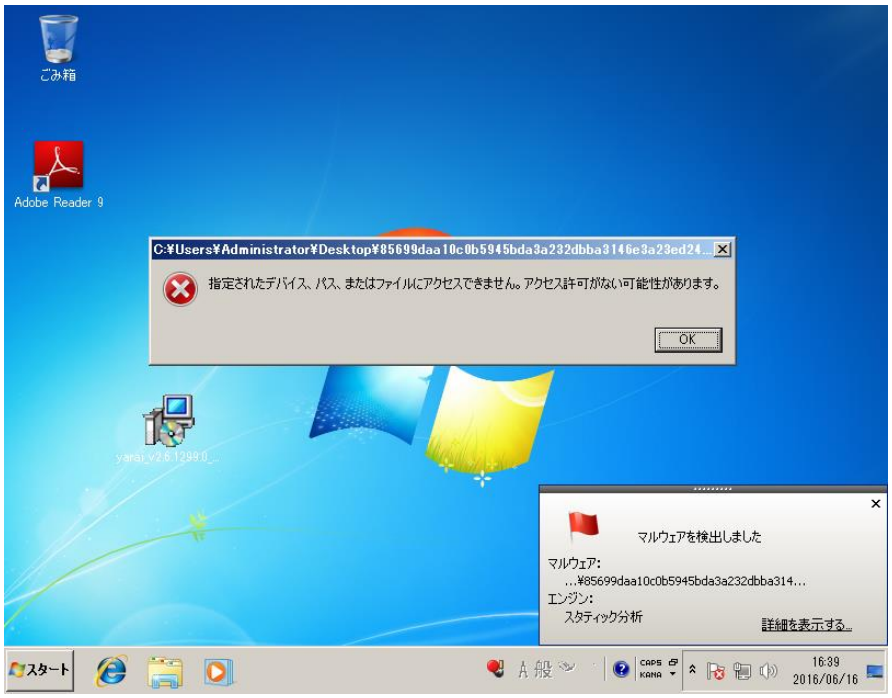
Windows 7 × FFR yarai 2.7.1437 (2016 年 3 月リリース)

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）

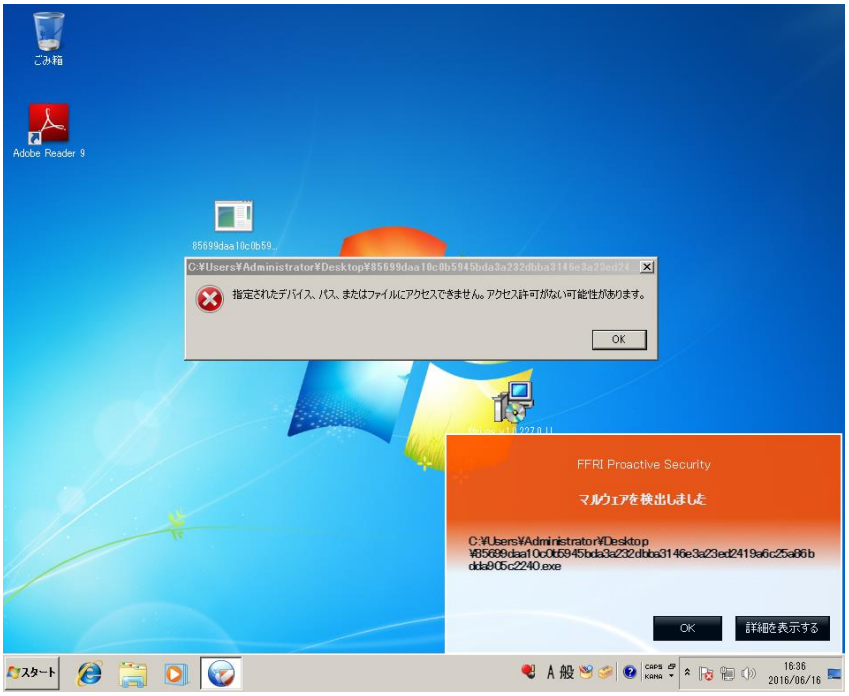
Windows 7 × FFRI プロアクティブ セキュリティ 1.1.395.2（2016 年 1 月リリース）

■検証した検体のハッシュ値

SHA256：85699daa10c0b5945bda3a232dbba3146e3a23ed2419a6c25a86bdda905c22



【FFR yarai 2.6.1299 検知画面】



【FFRI プロアクティブ セキュリティ 1.0.227 検知画面】

今回の検証で使用した FFR yarai 2.6.1299 と 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、各製品これ以降のバージョンをご利用いただいていた場合、攻撃を未然に防ぐことができたといえます。

なお、マルウェアには多くの亜種※2 が存在しており、今回の防御事例はそのすべての亜種を検知・防御可能であることを保証するものではありません。

※2 オリジナルのマルウェアを元に機能や構造を一部変更するなどして新たに生み出されるマルウェアのこと。最近ではサイバー攻撃者向けにマルウェア作成ツールが出回っており、このツールを使用することで簡単にマルウェアを作成できる状況にあり、マルウェアの数が急激に増加しています。

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）、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）、不正送金マルウェア「URLZone」（2016 年 2 月）、ランサムウェア「Locky」（2016 年 2 月）、ランサムウェア「PETYA」（2016 年 4 月）、自動解析を阻害するマルウェア（2016 年 4 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※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 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　経営企画部　IR 広報担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp

「ＦＦＲＩ」、「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。