報道関係者各位
プレスリリース

2015 年 12 月 8 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
ランサムウェア「TeslaCrypt（vvv ウイルス）」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 12 月 8 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）」がランサムウェア「TeslaCrypt（vvv ウイルス）」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。

ランサムウェア「TeslaCrypt（vvv ウイルス）」 vs. FFR yarai

2015 年 12 月上旬から、不正なバナー広告を表示しただけでランサムウェア※1 に感染したという被害報告が国内で相次いでいます。感染した場合には PC のハードディスクや外付けハードディスク上の多くのファイルが暗号化され、拡張子が「.vvv」に変更されます。暗号化されているため、拡張子を元に戻してもデータを復号しない限り使用することができません。また、Windows の復元ファイルも消されてしまうため、復元ファイルからの復旧も困難になっています。

※1 身代金要求ウイルスとも言われ、ユーザーのデータを人質にとり、データ回復のために身代金を要求するウイルス。

また、感染を引き起こす不正広告が正規サイトに表示されていることや、不正な広告と通常の広告を見分けることが難しいことなどが、感染をますます拡大させている一因になっていると見られます。

FFRI では今回問題となっている「TeslaCrypt（vvv ウイルス）」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 VISTA × FFR yarai 1.0.297（2009 年 5 月リリース）

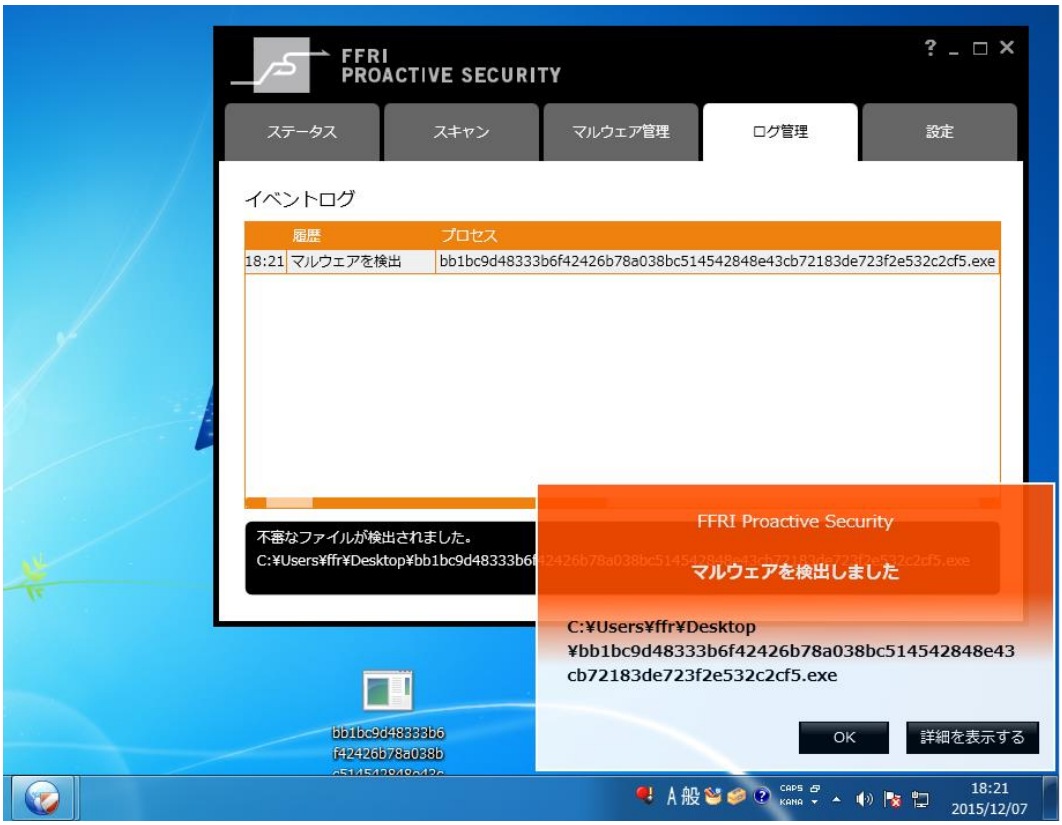
Windows 7 × FFRI プロアクティブ セキュリティ 1.0.206（2015 年 4 月リリース）

■検証した検体のハッシュ値（SHA-256）

bb1bc9d48333b6f42426b78a038bc514542848e43cb72183de723f2e532c2cf5

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の中のマルウェアの静的解析を担う Static 分析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 1.0.297 は 2009 年 5 月に、FFRI プロアクティブ セキュリティ 1.0.206 は 2015 年 4 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 2.6.1294（2015 年６月リリース）

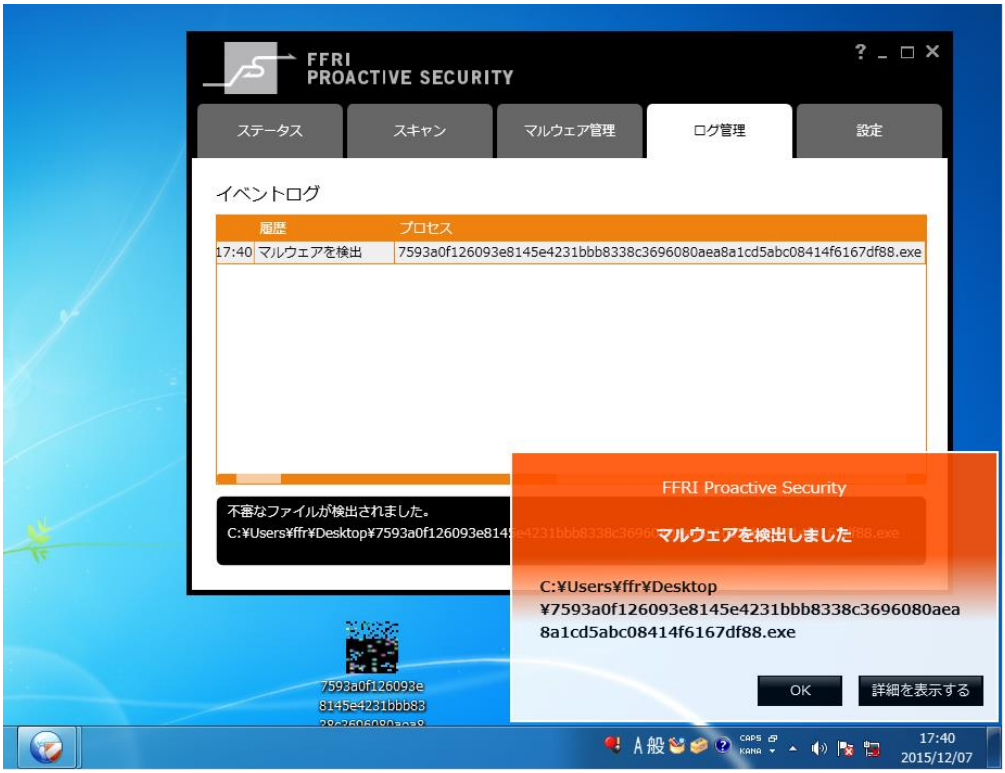
Windows 7 × FFRI プロアクティブ セキュリティ 1.0.206（2015 年４月リリース）

■検証した検体のハッシュ値（SHA-256）

7593a0f126093e8145e4231bbb8338c3696080aea8a1cd5abc08414f6167df88

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の中のマルウェアの動的解析を担う 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】



【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 2.6.1294 は 2015 年 6 月に、FFRI プロアクティブ セキュリティ 1.0.206 は 2015 年 4 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・マルウェアー覧

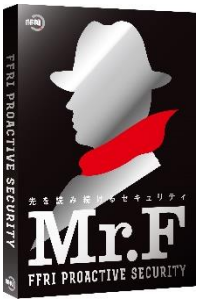
http://www.ffri.jp/products/yarai/defense_achievements.htm

◎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）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