報道関係者各位
プレスリリース

2017 年 5 月 15 日
株式会社ＦＦＲＩ

FFRI 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「WannaCry（WannaCrypt）」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、2017 年 5 月 15 日、標的型攻撃対策ソフトウェア「FFRI 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「WannaCry（WannaCrypt）」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「WannaCry（WannaCrypt）」 vs. FFRI yarai

2017 年 5 月 12 日ごろから Windows の古い脆弱性を悪用したランサムウェア「WannaCry（WannaCrypt）」の感染被害が世界 150 カ国以上で報道されています。英国では公共医療を管轄する国民医療サービスのシステムが一部地域で停止に追い込まれ、複数の医療機関で診療ができなくなるなどの混乱も生じています。日本国内でも被害が確認されたとの報道もあり、このランサムウェアの感染の拡大について IPA から緊急で注意喚起情報※1 が公開されています。

ランサムウェア「WannaCry（WannaCrypt）」が実行されると、Office 文書や動画、画像など 160 種類以上の拡張子のファイルが拡張子「.WNCRY」として暗号化され、身代金を要求する画面が表示されます。身代金の要求画面は日本語を含む多言語に対応しています。

ＦＦＲＩでは今回の攻撃に使われたランサムウェア「WannaCry（WannaCrypt）」の検体を入手し、標的型攻撃対策ソフトウェア「FFRI 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）」で検証したところ、ともに事件発生前にリリースしたバージョンで検知・防御が可能であることが確認できました。

※1 出典：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

【検証結果】

■検証環境

Windows 7 × FFRI yarai 2.7.8 (2016 年 10 月リリース)

Windows 7 × FFRI プロアクティブ セキュリティ 1.1.398.3(2016 年 9 月リリース)

■検証した検体のハッシュ値

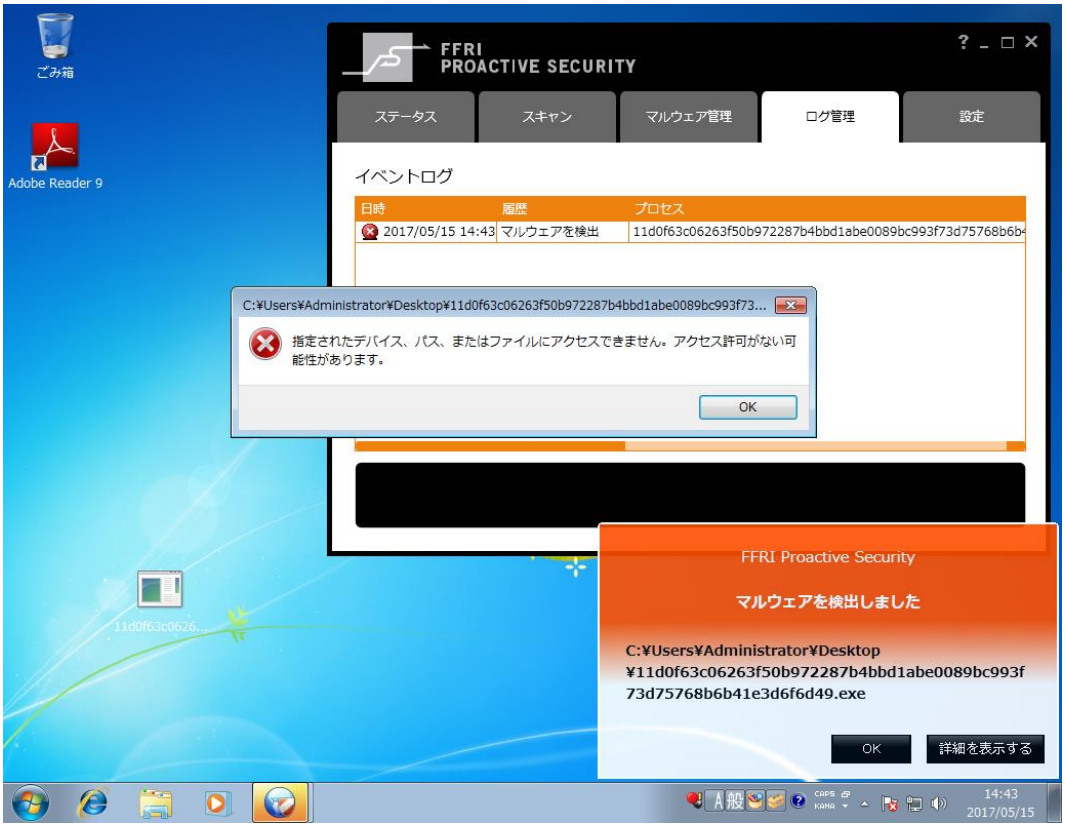
SHA256：

11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49

f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85

検証結果は、画面キャプチャのとおり、FFRI yarai 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。

【FFRI yarai 2.7.8 検知画面】



【FFRI プロアクティブ セキュリティ 1.1.398.3 検知画面】

今回の検証で使用した FFRI yarai 2.7.8（2016 年 10 月リリース）と FFRI プロアクティブ セキュリティ 1.1.398.3（2016 年 9 月リリース）は、ともに事件発生より半年以上前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では 2009 年の Gumbler ウイルス以降、メディアで報道された著名なサイバー攻撃やマルウェアの防御実績を当社 Web にて継続して公開しておりますが、本マルウェアについては検知がそれほど難しくないものでした。

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】

FFRI yarai

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

【FFRI yarai の防御実績】 これまでに防御した攻撃・マルウェア一覧

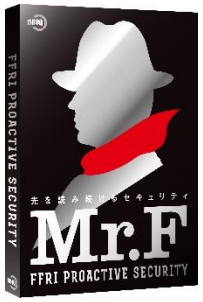
http://www.ffri.jp/products/yarai/defense_achievements.htm

◎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「FFRI yarai」とは

FFRI 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、「FFRI 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、ITR 調べ※4 による EDR 市場（2015 年度）における売上金額において No.1 を獲得しております。

※3 出典：「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 2016【外部攻撃防御型ソリューション編】」

※4 出典：ITR「ITR Market View：情報漏洩対策市場 2016」

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