報道関係者各位
プレスリリース

2016年4月15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
自動解析を阻害するマルウェアを検知・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、2016年4月15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、自動解析を阻害するマルウェア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。

自動解析を阻害するマルウェア vs. FFR yarai

ＦＦＲＩが2016年3月に入手した検体について検証・解析を行った結果、検体の解析を妨害する特徴としてアンチ VM※1 機能が見られました。

現在、ゲートウェイ型の標的型攻撃対策製品を中心に、サンドボックス技術により未知のマルウェアを検知するものがいくつかのセキュリティベンダーより販売されていますが、今回のようなアンチ VM 機能を搭載するマルウェアは、仮想環境では本来の動作をしない可能性が高く、サンドボックス型製品の検知をすり抜けてしまう恐れがあります。

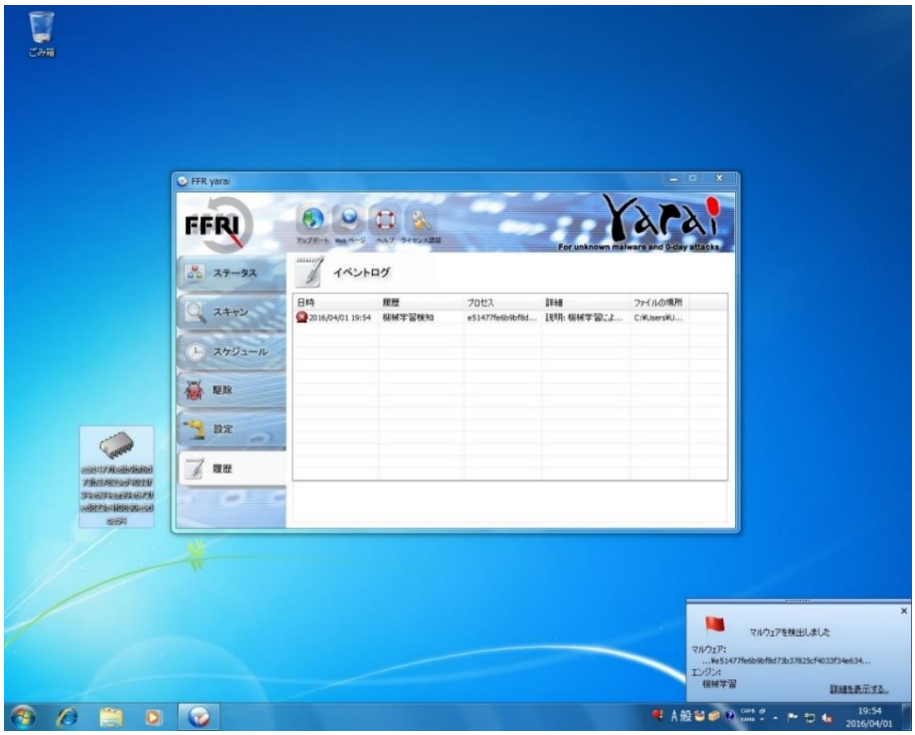
※1 自身が仮想環境で動いていると検知すると動作を停止するマルウェア。アンチ VM をはじめとした自動解析を阻害し、セキュリティ製品からの検知を免れるための自己隠ぺい技術は、最近ではインターネットバンキングユーザーを狙った不正送金マルウェア等にも見られます。

【検証結果】

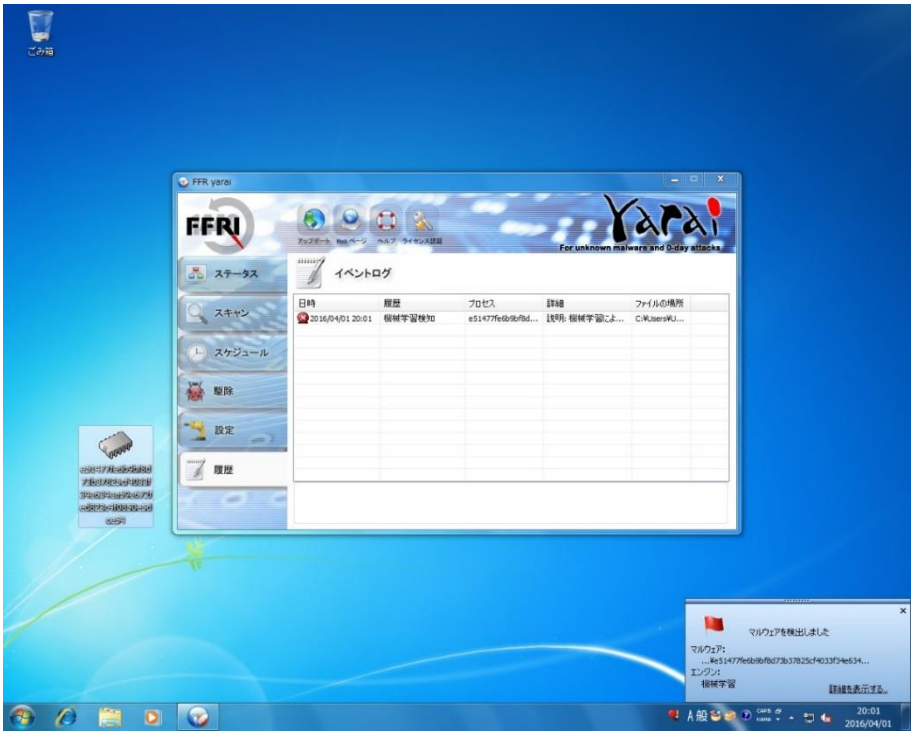
■検証環境
Windows 7 × FFR yarai 2.6.1299 (2015年7月リリース)
Windows 7 × FFR yarai 2.7.1437.5 (2016年3月リリース)
Windows 7 × FFRI プロアクティブ セキュリティ 1.1.395.2（2016年1月リリース）

■検証した検体のハッシュ値
SHA256：e51477fe6b9bf8d73b37825cf4033f34e634ea59e672fed823c4f0850e5dce54

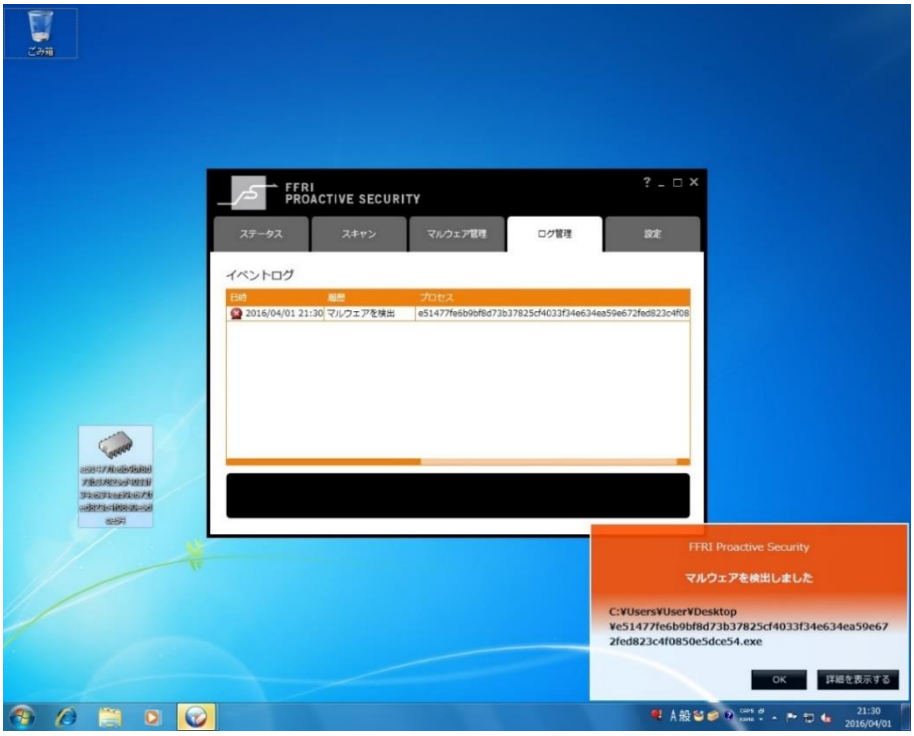
検証結果は、画面キャプチャのとおり、FFR yarai および FFRI プロアクティブ セキュリティの 5 つのヒューリスティックエンジンがマルウェアを検知してシステムを保護しています。



【FFR yarai 2.6.1299 検知画面】



【FFR yarai 2.7.1437.5 検知画面】



【FFRI プロアクティブ セキュリティ 1.1.395.2 検知画面】

今回の検証で使用した FFR yarai 2.6.1299 は 2015 年 7 月に、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、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。

【解析結果】

今回の検証で使用した検体について表層解析、動的解析、静的解析を行った結果、検体の解析を妨害する特徴としてアンチ VM※1 機能が見られました。攻撃者はマルウェアの発見や、マルウェアの解析者による解析を遅らせるために、マルウェアの解析を妨害する機能として仮想環境を検出するアンチ VM 機能などを実装しています。

マルウェアの解析を行う際には、マルウェアの挙動を容易に把握することが出来ることから、マルウェアを実際に動作させる動的解析と呼ばれる手法が用いられます。動的解析を行う場合、マルウェアを動作させるため、動作環境はマルウェアに感染してしまいますが、仮想環境で動作させることにより、容易に感染前の状態に戻すことが出来ます。アンチ VM 機能は仮想環境で動的解析されていることを検出し、仮想環境である場合には、本来の動作を行わないことにより、仮想環境での動的解析を妨害する機能です。

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 3 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