

報道関係者各位
プレスリリース

2015年3月26日
株式会社 FFRI



**従来のパターンマッチング型アンチウイルスソフトで防御不能な“未知の脅威”に対抗
FFRI、個人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」を4月1日リリース
～同日より「FFRI プロアクティブ セキュリティ発売開始記念キャンペーン」を実施～**

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：鶴飼裕司、以下 FFRI）は、2015年4月1日 10:00 より、個人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」の販売を『FFRI オンライン・ショップ』で開始いたします。また、新発売を記念し、特価でご購入いただけるキャンペーンも同日より実施いたします。

アンチウイルスソフトでは検知できないマルウェアが急増中

近年の急激に増え続けるマルウェア^{※1}による攻撃に対しては、従来のパターンマッチング型のアンチウイルスソフトだけでは対抗することが難しくなっています。最近では、悪意の第三者により日々膨大な数のマルウェアが作りだされており、アンチウイルスソフトは、パターンファイルの作成及び配信が追い付いていない状況です。さらに、高度なサイバー攻撃に使用されるマルウェアは、アンチウイルスソフトでは検知されない（パターンファイルに登録されていない）未知のマルウェアが使用されているという現実もあります。

このような状況の中、FFRI は現在法人向けに販売している「FFR yarai」^{※2}を個人向けにチューニングした、個人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」の発売を決定いたしました。

【製品名称】

FFRI プロアクティブ セキュリティ

【リリース日/価格】

ダウンロード1年版：2015年4月1日販売開始/

4月30日までのキャンペーン価格：7,000円（税抜）

5月1日以降：8,500円（税抜）

パッケージ1年版：2015年6月販売開始予定/8,500円（税抜）

【販売方法】

ダウンロード1年版：『FFRI オンライン・ショップ』よりダウンロード販売

FFRI オンライン・ショップ URL（4月1日オープン）：

http://www.ffri.jp/online_shop/index.htm

パッケージ1年版：店頭で販売予定



【キャンペーン概要】

名称：FFRI プロアクティブ セキュリティ発売開始記念キャンペーン

対象期間：2015年4月1日（水）10:00～4月30日（木）24:00

内容：上記対象期間内にFFRI オンライン・ショップ（http://www.ffri.jp/online_shop/index.htm 4月1日オープン）での購入処理が完了した方に、FFRI プロアクティブ セキュリティ（ダウンロード1年版）をキャンペーン価格でご提供いたします。

キャンペーン価格：7,000円（税抜）

※1 コンピュータ・ウイルス、スパイウェアなど、悪意のある目的を持ったソフトウェアやプログラムのこと。

※2 FFR yarai 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。

【FFR yaraiの防御実績一覧】http://www.ffri.jp/products/yarai/defense_achievements.htm

「パターンマッチング技術」と「ヒューリスティック技術」の違い

マルウェアの検知技術には大きく「パターンマッチング技術」と「ヒューリスティック技術」の2種類があります。「パターンマッチング技術」は、検査対象のプログラムと、パターンファイル（マルウェアのデータベース）をマッチングすることでマルウェアを検知・防御する仕組みです。アンチウイルスソフトベンダーは日々世界中からマルウェアを収集することでパターンファイルを作成し、ユーザーに配信しています。マルウェアのパターンファイルを保持していなければ検知することができないため、新種や改造されたマルウェアは検知・防御することができません。

「ヒューリスティック技術」はパターンファイルに全く依存せず、マルウェアの構造や振る舞いを見て、マルウェアに特徴的な「悪意」を分析することにより検知・防御する技術です。パターンマッチング技術では防御が難しい新種や改造されたマルウェアであっても、マルウェアに共通する「悪意」を検知して防御することが可能です。

未知のマルウェアに対応する「プログレッシブ・ヒューリスティック技術」

FFRI プロアクティブ セキュリティでは、FFRIが独自に開発したプログレッシブ・ヒューリスティック技術により、既知・未知に関係なく、マルウェアの脅威から防御します。

単一的なアプローチによるヒューリスティック分析では、検知精度が不十分なために、本来検知すべきマルウェアを検知できなかったり、正常なプログラムを誤検知してしまう懸念がありました。FFRI プロアクティブ セキュリティは、攻撃者の思考を先回りした先進的な検知ロジックを複数搭載するプログレッシブ・ヒューリスティック技術で検査対象のプログラムを多角的なアプローチで分析し、マルウェアをリアルタイムで高精度に検知・防御します。

【FFRI プロアクティブ セキュリティのプログレッシブ・ヒューリスティック技術】

アプリケーションを脆弱性攻撃から守る

ZDPエンジン

マルウェアを検出する

Static分析エンジン

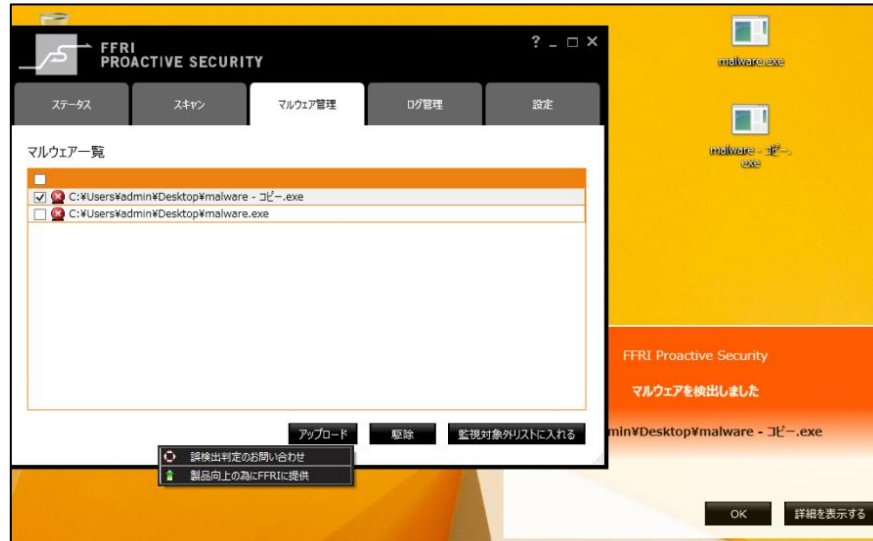
Sandboxエンジン

HIPSエンジン

機械学習エンジン

■ ZDPエンジン	メールやWebページ閲覧時の攻撃など、既知・未知の脆弱性を狙ったウイルス攻撃を防御。独自の「API-NX」技術(特許第4572259号)で、任意コード実行型脆弱性の攻撃を防御。
■ Static分析エンジン	プログラムを動作させることなく分析。「PE構造分析」「リンカー分析」「バッカー分析」「想定オペレーション分析」など多数の分析手法「N-Static分析」で検知。
■ Sandboxエンジン	仮想CPU、仮想メモリ、仮想Windowsサブシステムなどで構成される仮想環境上でプログラムを実行。独自の「U-Sandbox検知ロジック」で命令の組み合わせに基づいて検知。
■ HIPSエンジン	実行中プログラムの動作を監視。他プログラムへの侵入、異常なネットワークアクセス、キーロガーやバックドア的な動作などの挙動を、独自の「DHIPSロジック」で検知。
■ 機械学習エンジン	FFRIが収集したマルウェアに関するビッグデータを元に実行中のプログラムを監視。ビッグデータ上の振る舞い特性を抽出し、機械学習で分析した特徴により端末上の悪意ある挙動を検知。

【画面イメージ】



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 2014【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・資料等をご入用の場合もお問い合わせください。

株式会社 FFRI
経営企画部 PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp URL：<http://www.ffri.jp>

「FFRI」、「FFR yarai」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。