報道関係者各位
プレスリリース

2017 年 8 月 31 日
株式会社ＦＦＲＩ

ＦＦＲＩ、マルウェア自動解析ツール「FFRI yarai analyzer Version1.6」「FFRI yarai analyzer Professional Version1.2」をリリース
～最新の FFRI yarai のエンジンを搭載し、ファイルレスマルウェア対策を強化～

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、マルウェア自動解析ツール「FFRI yarai analyzer Version1.6」および「FFRI yarai analyzer Professional Version1.2」の出荷を 2017 年 8 月 31 日より開始いたします。

高度なマルウェア攻撃の解析

これまで主要なマルウェア検出技術は、主に実行ファイルを対象としてきましたが、昨今はショートカットの利用やマクロ、スクリプトをトリガーとする「ファイルレスマルウェア」の攻撃も確認されるようになり、今後のマルウェア検出技術は、より広範囲な種類のファイルを対象としていくことが求められています。さらにファイルレスマルウェアを利用した攻撃は、インシデント発見後においても痕跡が残りづらいことから、ふるまい検知を利用した動的な解析が求められます。今回のバージョンアップでは、ファイルレスマルウェアの検知※1を強化した今年５月にリリースした最新の FFRI の標的型攻撃対策ソフトウェア「FFRI yarai」のエンジンを新たに搭載しています。

※1　【FFRI BLOG】FFRI yarai がファイルレスマルウェアを検知
http://www.ffri.jp/blog/2017/07/2017-07-25.htm

セキュリティ人材不足を補うテクノロジー

CSIRT/SOC を自社内に組織する企業や団体の数も伸びてきている※2一方で、セキュリティ人材が不足している状況が続いています。新種マルウェアの発生件数増加や、標的型攻撃などで利用される個別にカスタマイズされた未知のマルウェアの存在により、アンチウイルスベンダーではマルウェア検体の入手も困難で、パターンファイルの作成や対策に必要な情報をタイムリーに提供できないケースも増加しています。こうした状況も踏まえ、CSIRT/SOC 担当者から「疑わしいファイルのマルウェア判定を組織内部で迅速に判断したい」、「マルウェアの影響範囲を組織内部で把握し、対策方法を迅速に検討したい」といった声もＦＦＲＩに寄せられています。

※2　日本シーサート協議会　会員となっているチームは 242 チーム（2017 年 8 月 1 日現在）
http://www.nca.gr.jp/member/index.html

「FFRI yarai analyzer」および「FFRI yarai analyzer Professional」は、マルウェアと疑わしきファイルを任意の検査フォルダに置くだけで自動的に解析が実行され、解析結果レポートを出力します。お客様はマルウェア解析のための専門知識を必要とせず、簡単・迅速にマルウェアの危険性や影響を把握できるため、外部ベンダーに依存しない自己完結型のインシデントレスポンス体制の強化が可能です。また、標的型攻撃対策製品として高い評価を受けている「FFRI yarai」のプログレッシブ・ヒューリスティック技術を用いた検知エンジンを搭載しており、未知マルウェアや 0-day 脆弱性攻撃を高精度で検出します。実績としては、大手製造業での製品出荷前検査におけるマルウェア混入チェックや、法執行機関でのマルウェア解析、豊島区役所様でのメール添付ファイルのマルウェア検査
http://www.ffri.jp/assets/files/products/exp/yarai_analyzer_toshima.pdf
などにご利用いただいております。

今回のバージョンアップでは、解析エンジンのアップデートによってマルウェア検出力を強化したほか、対応ゲスト OS の拡充も行っています。

【FFRI yarai analyzer Version1.6 の新機能】
【FFRI yarai analyzer Professional Version1.2 の新機能】

●解析エンジンの強化

- ファイルレスマルウェア対策を強化し、機械学習エンジンを刷新した FFRI yarai Version2.9 のエンジンを搭載し、マルウェア検出力を強化

●対応ゲスト OS の拡充

- 下記のゲスト OS に対応
  ・Windows 10 32bit/64bit
  ・Window Server 2003 SP2 以降 (32bit) / 2003 R2 SP2 以降 (32bit)
  ・Windows Server 2008 (32bit/64bit) / 2008 R2 (64bit)
  ・Windows Server 2016 (64bit)

【製品名称】

FFRI yarai analyzer Version1.6

◆製品ページ

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

◆導入事例ページ（豊島区役所様）

http://www.ffri.jp/assets/files/products/exp/yarai_analyzer_toshima.pdf

【製品名称】

FFRI yarai analyzer Professional Version1.2

◆製品ページ

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

【リリース日】

2017 年 8 月 31 日

■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、IT 社会に貢献すべく設立されました。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：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 2017【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