報道関係者各位
プレスリリース

2016 年 4 月 6 日
株式会社ＦＦＲＩ

攻撃者の意図を分析し、サイバー攻撃対策のスピード化とコスト削減を実現
マルウェア自動解析システム「FFR yarai analyzer Professional Version1.1」をリリース
～検体実行時に生成されたファイルの取得機能、ゲスト OS の多言語対応～

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システム「FFR yarai analyzer Professional Version1.1」の出荷を 2016 年 4 月 6 日より開始いたします。

マルウェア解析者の負担を大幅に軽減し、迅速なサイバー攻撃対策の検討を支援

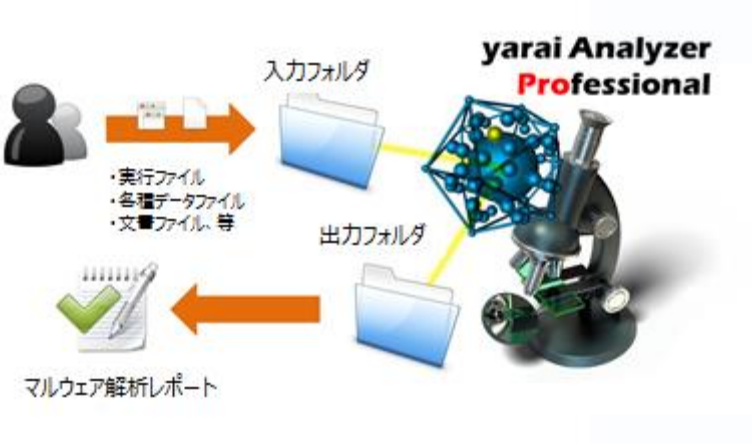
サイバー攻撃は急速に巧妙化しているため、対応が遅れると、被害がさらに拡大してしまいます。また、その原因を確実に突き止めなければ、再度攻撃の対象になる可能性もあります。

これまで多くの企業や団体において、マルウェアの発見後、その対応が遅れがちになっていた理由のひとつに、解析をアンチウイルスベンダーに依頼しなければならず、調査レポートの納品までに数日を要するといった問題がありました。

FFR yarai analyzer Professional は、検査対象ファイルやフォルダを静的/動的な手法で自動解析し、HTML 形式でレポートを出力する、マルウェア自動解析システムです。アンチウイルスベンダーに依頼せずに、社内でマルウェアがどのような挙動を行うのかを解析できるため、攻撃者の意図を分析し、効率的に対策を打つことが可能です。

マルウェア解析者の負担を大幅に軽減するため、FFR yarai analyzer Professional には、解析結果を IDA（マルウェアのリバースエンジニアリング時に使用する逆アセンブラツール）にインポートする機能、プロセス・スレッドの相関分析機能、Anti-VM や時限式マルウェア等の解析対策機能を持つマルウェアを解析するための機能等を備えています。

【FFR yarai analyzer Professional を利用したマルウェア解析のイメージ】



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、SOC 等でゲストOSの状態を複数管理するニーズに対応してスナップショット指定機能を追加、解析対象から生成されたファイルも解析対象とするニーズを受け、検体実行時に生成されたファイルの取得機能も追加しました。また、対応ゲスト OS の拡充・多言語対応やレポート・管理機能の強化も行っています。

【FFR yarai analyzer Professional Version1.1 の新機能】

●解析エンジンの強化

- FFR yarai Version2.7 のエンジンを搭載し、マルウェア検出力を強化

●スナップショット指定機能の追加

- SOC 等での利用においてゲスト OS の状況を変化（セキュリティ更新プログラム適用の有無、ソフトウェアのバージョン等）させながらマルウェア解析するケースにも対応
  ・ゲスト OS の状態を複数管理可能
  ・Controller.conf にスナップショット名を指定することで、指定のスナップショットにリバートし、解析を実行

●検体実行時に生成されたファイルの取得機能を追加

- 検体実行時にサーバからダウンロードまたは内部のリソース等からファイルが生成されて実行された場合、生成されたファイルをプロセスごとにフォルダ分けして出力

●対応ゲスト OS・仮想環境の拡充

- 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 2012 (64bit) / 2012 R2 (64bit)
- 下記の仮想環境に対応
  ・VMware vSphere 6.0
  ・VMware Workstation 12.x Pro

●ゲスト OS の多言語対応

- 特定の言語環境下でしか動作しないマルウェア解析用に下記の言語に対応
  ・英語版
  ・中国語版（簡体字、繁体字）
  ・ロシア語版

●レポート・管理機能の強化

- ハッシュ値、埋め込まれている文字列、パッカー情報、デジタル署名情報、バージョン情報、Virus Total へのリンクを追記

【製品名称】

FFR yarai analyzer Professional Version1.1

【リリース日】

2016 年 4 月 6 日

◆製品ページ

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

■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、「FFR yarai」はミック経済研究所調べ※1 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。

※1　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