報道関係者各位
プレスリリース

2014 年 1 月 16 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
FFRI、マルウェア自動解析システム「FFR yarai analyzer Professional」をリリース
～解析結果をIDA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を搭載～

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」の出荷を 2014 年 1 月 16 日より開始いたします。

高度なマルウェアを容易に作成できるツールの流通が、サイバー攻撃を加速

企業や学校、官公庁等を狙った Web サイトの改ざんが急増しています。改ざんされたWebサイトを閲覧した PC をマルウェアに感染させる、ドライブ・バイ・ダウンロード攻撃に利用されているのが、Exploit Kit または Exploit Pack と呼ばれるマルウェア作成ツールです。これらのツールは、アンダーグラウンドマーケットで売買されており、パッケージ化され、さまざまな脆弱性への攻撃に対応しているため、標的システムのセキュリティ対策技術をすり抜ける、高度なマルウェアを容易に作成できるようになってきていることが、サイバー攻撃をより加速させています。

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

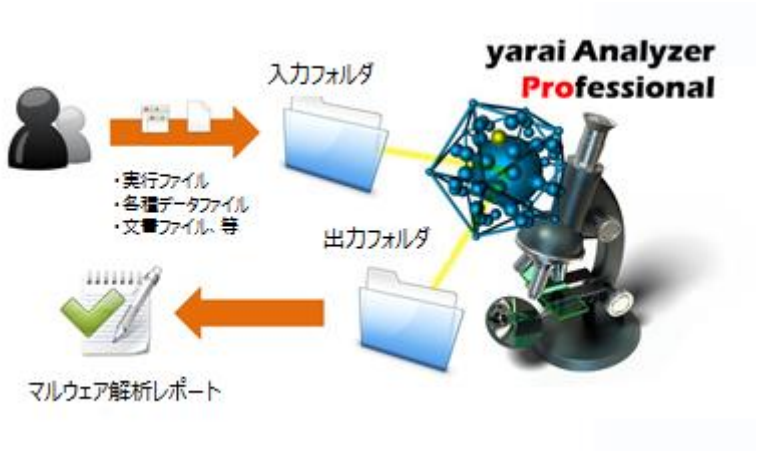
サイバー攻撃は急速に高度化しているため、対応が遅れると、被害がさらに拡大してしまいます。また、その原因を確実に突き止めなければ、再度攻撃の対象になる可能性もあります。

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、社内でマルウェアか否かがすぐに判定できます。判定の結果、マルウェアであった場合は、マルウェアがどのような挙動を行うのかを解析することで、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】



【FFR yarai analyzer Professional の特徴】

●柔軟なカスタマイズが可能な解析環境で自動解析

- 任意の解析用ディレクトリに検査対象のファイルやフォルダを設置するだけで自動的に解析を実行。検査対象ファイルが実行された際に、新たに生成されたファイルや外部からダウンロードされたファイルも自動的に解析。
- 特定の環境下でしか動作しない脆弱性攻撃やマルウェアの解析に対応するため、解析環境の OS やアプリケーションを自由に構築（解析環境上の OS/アプリケーションのライセンスは別途必要）し、検査対象ファイルの拡張子毎に処理ルールの設定が可能。
- 最大 6 つの解析環境で、同一ファイルを同時に検査可能。

●未知の脆弱性攻撃やマルウェアへの対応

- 解析環境には標的型攻撃対策として実績のある FFR yarai のヒューリスティックエンジンを搭載。静的/動的な解析を実施し、既知・未知に関係なく、脆弱性攻撃やマルウェアを検出。

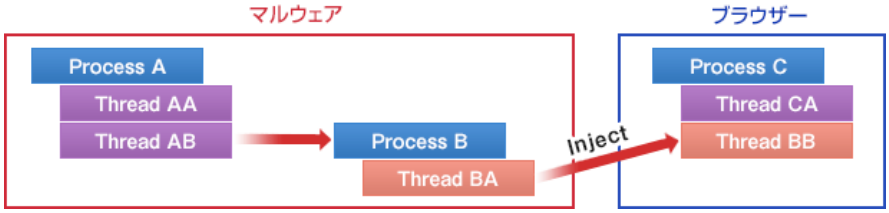
●解析者の負担を減らす機能の数々

- API 呼び出し履歴解析機能

  FFR yarai analyzer Professional の動的解析により、マルウェアが呼び出した API を記録し、時系列でレポートすることが可能なため、静的解析では得られない詳細な挙動を把握可能。
- 解析結果を IDA にインポートする機能

  FFR yarai analyzer Professional の動的解析により実際にマルウェアを動作させた結果等をコメントとして IDA にインポート可能。
- 検査対象ファイルの実行により生成されたプロセスとスレッドの相関分析機能

  従来、デバッガーによる動的解析でしか得られなかったマルウェアの詳細な挙動（生成されたプロセスとスレッドの関係）を可視化し、わかりやすくレポート。



- 解析対策機能を持つマルウェアを解析する機能やツール

  ・Anti-VM 対策

  解析システムの存在を想定し、自身が仮想環境で動作していることを検知すると、動作を停止するマルウェアも解析可能。

  ・時限式マルウェア対応

  特定の日時にマルウェアとして動作を開始する時限式マルウェアへの対応として、解析環境のシステム時間を進行させる機能を実装。

  ・疑似環境ツールの提供

  特定の環境でしか動作しないマルウェアを解析するために、マルウェア自身の実行ファイルパスやシステムドライブの GUID を解析環境に設定するための疑似環境ツールも提供。

●日本語によるわかりやすい解析結果

- 解析結果は HTML 形式で出力され、ハッシュ値、ファイルサイズ、マルウェア判定結果、ファイル変更履歴、レジストリ変更履歴、ネットワークアクセス履歴などの情報を日本語で表示。

【製品名称】

FFR yarai analyzer Professional

【リリース日】

2014 年 1 月 16 日

【参考価格(税別)】

20,000,000 円 ※1

※1 物理マシン 1 台につき、1 ライセンス必要となります。物理マシン 1 台につき、利用可能な Crawler は 6 つまで、Controller は 1 つまでとなります。初年度の保守費用は、ライセンス価格に含まれております。次年度以降の保守費用は、ライセンス価格の 20%となります。

◆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※2 および富士キメラ総研調べ※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。

※2　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 2013【外部攻撃防御型ソリューション編】」

※3　出典：富士キメラ総研「2013 ネットワークセキュリティビジネス調査総覧【上巻 市場編】」

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
コーポレートコミュニケーション部　PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　　URL：http://www.ffri.jp