株式会社ＦＦＲＩセキュリティ

FFRI yarai analyzer Professional

マルウェア解析に必要な高度な分析作業を自動化

マルウェア解析で得られた情報から攻撃者の意図を分析し、効果的な対策を実現

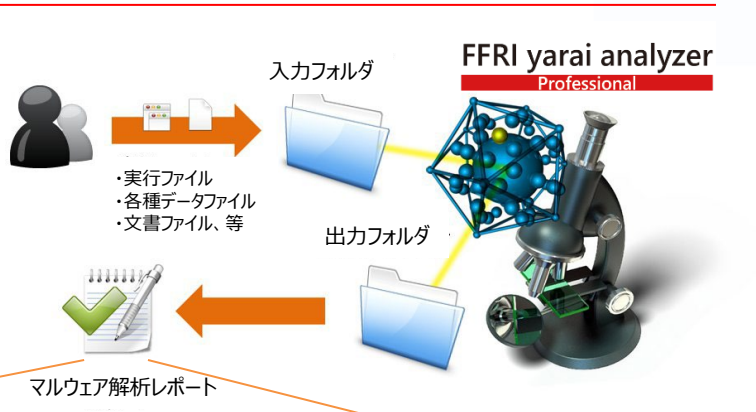
近年、攻撃者のネットワークが国際的に組織化され、サイバー攻撃の技術が急速に高度化しています。また、それらの高度な攻撃技術がExploit Kitやマルウェア作成ツールとして汎用化され、アンダーグラウンドマーケットで流通することにより、高度な技術を悪用したサイバー攻撃が従来よりも容易に実現できる状況となっています。特定の企業や組織をターゲットとした標的型攻撃では、攻撃者がこれらの攻撃ツールを利用して標的システムのセキュリティ対策技術を掻い潜るための独自マルウェアを作成し、ターゲットに送り込みます。

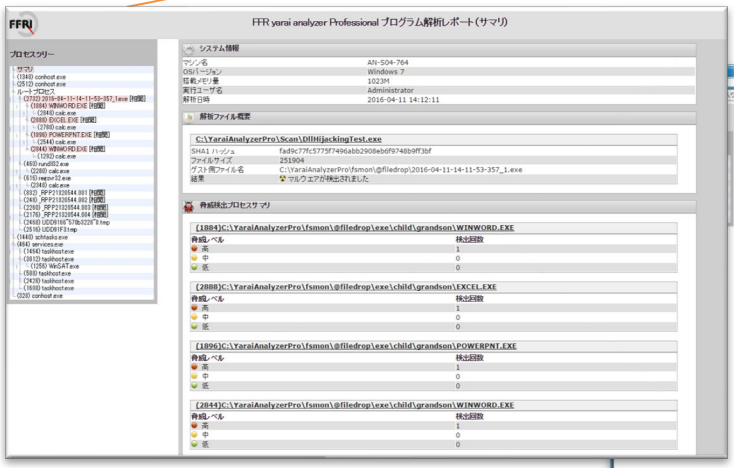
FFRI yarai analyzer Professional は、プログラムファイルや文書ファイル、各種データファイルといった検査対象ファイルを静的/動的な手法で自動解析し、解析結果をHTML形式でレポート出力します。FFRI yarai analyzer Professional を使って、巧妙な手法で組織内に送り込まれたマルウェアがどのような挙動を行うのかを解析することで、攻撃者の意図を分析し、効果的な対策を実現することが可能となります。

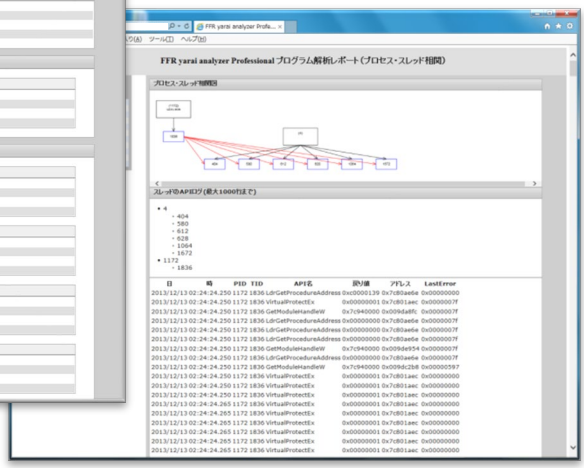
FFRI yarai analyzer Professional を利用したマルウェア解析のイメージ

Step 1：検査対象ファイルの投入
検査対象ファイル（exeファイルや、PDF、WORD等の文書ファイル、各種データファイル）をFFRI yarai analyzer Professional で検査用に指定したディレクトリに投入。

Step 2：レポート閲覧
HTML形式の解析レポートがFFRI yarai analyzer Professional のレポートフォルダに生成。Webブラウザーで閲覧。







FFRI yarai analyzer Professional

FFRI yarai analyzer Professional の特徴

仮想化技術を利用した解析環境

解析環境で実行したファイルのAPI呼び出しを監視し、挙動をリアルタイムに検出。任意の解析用ディレクトリに対象のファイルやフォルダを設置するだけで、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解析。

未知の脅威への対応

解析環境には標的型攻撃対策製品として実績のあるFFRI yaraiの5つのヒューリスティックエンジンを搭載。静的/動的/半動的解析を実施し、既知・未知に関係なく、脆弱性攻撃やマルウェアを検出。

AntiVM機能を持つマルウェアの解析

FFRI yarai analyzer Professional は、AntiVM対策の設定をVMwareに実施しても、マルウェアを解析することが可能。

解析環境のカスタマイズ

解析環境のOSやアプリケーションを自由に構築し、検査対象ファイルの拡張子毎に処理ルールの設定のほか、最大6つまでの解析環境を用意し、同一ファイルをそれぞれの解析環境で検査することも可能。

※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

わかり易い解析結果

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が日本語で表示。

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や、解析結果をIDAにインポートする機能、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関係の可視化が可能。

■仮想環境にHyper-Vを使用可能

仮想環境に、Microsoftが提供するHyper-Vを追加VMWare製品に替わる選択肢をご提供いたします。

■サブスクリプション型で導入可能

売り切り型の他、月額ごとの料金プランでイニシャルコストを抑えた導入が可能です。
詳しくは販売店までお問い合わせください。

動作環境

■推奨スペック

【YAController(ホストOS)】
CPU：Intel Core i5 相当以上
メモリ：8GB以上
HDD：100GB以上
【YACrawler(ゲストOS)】
CPU：1つ以上(VMware上での割り当て個数)
メモリ：2GB以上
HDD：20GB以上

※ControllerとCrawlerを同一マシン上に構築する場合、物理マシンのスペックとしてはControllerとCrawlerのスペックを足し合わせたものにすることを推奨

■推奨スペック（VMware vSphere を用いた場合）

【仮想環境】
HW：VMware vSphere がサポートするハードウェア
CPU：VMware vSphere がサポートするCPU
メモリ：16GB以上推奨
HDD：500GB以上推奨
【YAController(ホストOS)】
CPU：4つ以上(VMware上での割り当て個数)
メモリ　：8GB以上
HDD　：100GB以上
【YACrawler(ゲストOS)】
CPU：1つ以上(VMware上での割り当て個数)
メモリ：2GB以上
HDD：20GB以上

仮想環境

VMware Workstation Pro 17
VMware vSphere 7 / 8
Microsoft Hyper-V

※Vmware社の各製品は VMware のサポート終了時に FFRI yarai analyzer Professionalのサポート対象外となります。

対応OS

■YAController（ホストOS）

Windows Server 2016（64bit）日本語版
Windows Server 2022（64bit）日本語版

■YACrawler（ゲストOS）

Windows 10 22H2 日本語版（64bit）
Windows 11 23H2 日本語版（64bit）
Windows 11 24H2 日本語版（64bit）
Windows Server 2016（64bit）日本語版
Windows Server 2022（64bit）日本語版
※FFRI yarai analyzer Professional 専用に構築したシステムのみをサポート対象

※HDDの空きディスク容量について 最小スペック、推奨スペックに記載の空きディスク容量には、OSのインストールに必要な容量は含まれておりません。
推奨スペックに記載の空きディスク容量の他にOSのインストール用の容量が必要となります。
※当社サポートサービスでは、FFRI yarai analyzer Professionalを用いてお客様が解析したファイルについて、過検出の判定も含めてマルウェア解析に関する回答は実施しておりません。
※サポート期間の詳細については、下記URLを御覧ください
https://www.ffri.jp/products/yarai_analyzer_pro/yarai_analyzer_pro_requirement

製品・サービスについてのお問い合わせは
株式会社ＦＦＲＩセキュリティ
〒100-0005
東京都千代田区丸の内3-3-1　新東京ビル2階
TEL：03-6277-1811　E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。
https://www.ffri.jp/

2025年5月現在
Ver. 2.00.24