Yarai Analyzer

Automated Malware Analysis System

簡単・迅速。マルウェアを自動分析

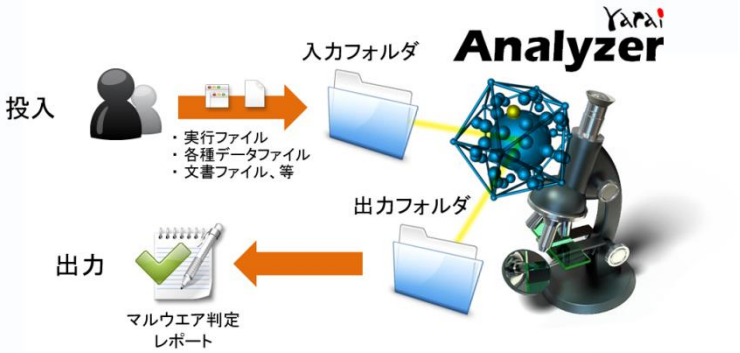
不審ファイル発見時の初動分析、ハッキングによる情報流出対策など、さまざまなマルウェア解析シーンで活用可能。

近年、ハッカーは国際的に組織化され、攻撃のテクノロジーは急速に高度化。マルウェアは増加の一途をたどっており、一日あたりの発生件数は数十万あるいは百万以上とも言われています。また、セキュリティ脆弱性を悪用したマルウェアも急増しており、近年では未修正(0-day)の脆弱性を悪用するケースも多発しています。このため、近年の新しいマルウェアの多くは、既存の仕組みで検知できない状況が続いています。

FFRI yarai analyzerは、通常高度な知識と専門性が必要となるマルウェアの解析を自動化し、マルウェアの挙動を詳細にレポートします。また、FFRI yarai のヒューリスティックエンジンを搭載しているため、未知マルウェア、0-day脆弱性といった、未知の脅威も分析することが可能です。

Step 1：検査対象ファイルの投入
検査を実施したいWindows実行ファイル(exeファイル等)や、PDF等の文書ファイル、各種データファイルをFFRI yarai analyzer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のレポートフォルダーに生成。Webブラウザーで閲覧。



FFRI yarai analyzer の活用シーン

初動マルウェア解析
マルウェアが組織内で発生した際、情報漏洩やシステム破壊が発生する可能性があるため、適切な対応が求められています。マルウェアの被害を素早く分析し、対応方針の決定を支援します。

メール添付型マルウェア、標的型メール攻撃検知センサー
近年、ハッキングによる情報漏洩が相次いでいます。メール解析システムとの連携により、メール添付型マルウェアや標的型攻撃を検知できます。メール経由でのハッキングによる情報漏洩を可視化します。

社内持込み外部デバイス検査
USBメモリなどを社内に持込む際に事前検査します。社外でマルウェアに感染した場合でも、マルウェアの感染拡大を防止します。

SOC運用支援
スナップショット指定機能を活用することで、ゲストOSの状態を複数管理可能となります。組織内で異なる環境下にて各端末が使用されている場合でも、解析対象となるゲストOSの状態を指定することで、特定の環境下での解析を実施できます。

入力されたファイルを自動解析、解析レポートはHTML形式で日本語出力（XML形式にも対応）

図1：解析レポート(サマリ)

FFRI yarai analyzerは入力されたファイルを解析したのち、解析レポートを出力します。解析レポートは、対象ファイルを実行した際にアクセスしたファイルシステム情報、レジストリ情報、ネットワーク情報などを出力するサマリページ(図1)のほか、サマリページに表示される各プロセスをクリックすることで表示されるプロセス詳細レポート(図2)の2種類存在します。

わかり易いサマリレポート

図1の解析レポート(サマリ)ではシステム情報や解析ファイル概要のほか、脅威検出プロセスサマリ、ネットワークのアクセスサマリなどの各種情報が日本語で表示。

脅威を可視化する詳細レポート

図2の解析レポート(プロセス詳細)では、検出した脅威の詳細説明のほか、各プロセスから行われたファイルの更新情報やネットワークアクセス情報などの各種更新情報を日本語で出力し、インシデント後の対応を支援。

ver.1.8新機能

■**解析エンジンを強化**

昨今流行しているマルウェアの解析能力を向上

.lnkマルウェア対策強化

コマンドラインの難読化（DOSfuscation）対策強化

耐解析機能を持つマルウェア対策を強化など

■**VMware vSphere 6.7に対応**

図2：解析レポート(プロセス詳細)

動作環境

■推奨スペック
※Controller 1台、Crawler 3台を動作させることを想定

【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： 1GB以上(32bitの場合)
2GB以上(64bitの場合)
HDD：16GB以上(32bitの場合)
20GB以上(64bitの場合)

※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）
※Controller 1台、Crawler 3台を動作させることを想定

【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(6Core以上推奨)
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： 1GB以上(32bitの場合)
2GB以上(64bitの場合)
HDD：16GB以上(32bitの場合)
20GB以上(64bitの場合)

仮想環境

VMware vSphere 6.0 ＋ VIX API 1.14VMware
Workstation Pro 15.x ＋ VIX API 1.17
VMware vSphere 6.7 ＋ VMware PowerCLI 注1
※上記の製品は VMware のサポート終了時に FFRI yarai analyzer のサポート対象外となります。
注１製品で使用するVMware PowerCLIのモジュールは、製品のインストーラに同梱されているため、別途インストール作業は不要です。

対応OS

■YAController（ホストOS）

Windows Server 2012（64bit）日本語版
Windows Server 2012 R2（64bit）日本語版
Windows Server 2016 (64bit) 日本語版
※.NET Framework 4.5以上、4.7以下のバージョンがインストールされていること
※Windows Server 2012 R2は以下のKBの適用が必要
- KB2919355

■YACrawler（ゲストOS）

Windows 7 SP1以上 （32bit, 64bit）
Windows 8.1 （32bit, 64bit）
Windows 10 （32bit, 64bit）
Windows Server 2012 （64bit）
Windows Server 2012 R2 （64bit）
Windows Server 2016 （64bit）
※FFRI yarai analyzer専用に構築したシステムのみをサポート対象
※YAController(ホストOS)とYACrawler(ゲストOS)の双方で、下記のOSに記載のサービスパック、またはアップデートの適用が必要です。
・Windows 8.1 とWindows Server 2012 R2は、以下のKBを適用が必要
- KB2919355
※上記日本語OSのみ対応

※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 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/requirement.htm 5

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/

■このパンフレットの内容は改良のために予告無しに仕様・デザインを変更することがありますのでご了承ください。

2020年1月現在
Ver. 2.00.25