標的型攻撃マルウェア検査サービス

標的型攻撃マルウェア検出専用の高感度エンジンで端末を調査。マルウェア解析を実施し、実被害を分析。

標的型攻撃マルウェアの感染有無を調査。リスクを分析。

近年、機密情報の取得などを目的とした「標的型攻撃」が多発しています。標的型攻撃による機密情報漏洩は、時に、事業継続上重大なインシデントとなる事がありますが、既存の技術では発見・防御が困難であり、そのリスクが表面化しにくい状況です。

標的型攻撃では、攻撃対象にピンポイントでマルウェアを送り付けるため、既存のパターンファイルをベースとしたウイルス対策製品では検知できない場合が殆どです。このため、標的型攻撃はさまざまなサイバー脅威の中で「最も見えにくい脅威」の一つと言われています。

「標的型攻撃マルウェア検査サービス」では、標的型攻撃マルウェアの検出に特化した高感度の専用検出エンジンを用いて、ネットワーク内から標的型攻撃マルウェアを洗い出します。

- 標的型攻撃マルウェアが存在するのか否か
- そのマルウェアが何を行い、どのような被害が発生しているのか
- 懸念されている被害で発生していないものは何か

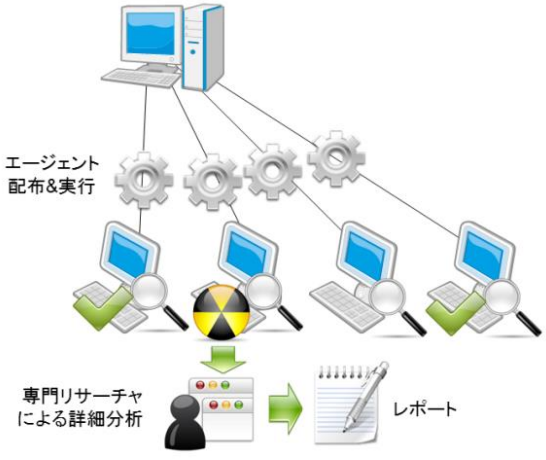
被害が発生している場合は対策立案や外部への報告・発表を含めた事後対応を強力にサポートします。
「標的型攻撃マルウェア検査サービス」では、標的型攻撃による機密情報漏洩のリスクを可視化し、対策検討含め、標的型攻撃に対する適切なリスク管理の実現を支援します。

端末にエージェントを配布・実行。ログファイルと疑陽性ファイルを解析。

標的型攻撃は、主にクライアント端末が攻撃対象となります。このため、主にクライアント端末が検査の対象となります。端末にエージェント（実行ファイル）を配布・実行し、ファイルシステム内をスキャンします。

エージェントは、FFRI yarai のエンジンをベースに、標的型攻撃検出に特化したチューニングを施したものであり、高い感度でマルウェアの疑いがあるファイルを収集します。エージェントは高い感度で収集を行うため、通常のファイルも含まれる事があります。このため、専門アナリストが収集されたファイルの概要調査を実施します。

マルウェアの疑いが強いものについては検出された端末やファイル情報などをご報告します。マルウェアの疑いが強いと判定されたファイルについては、専門アナリストが詳細解析(リバースエンジニアリング)を実施し、脅威分析を行います。



標的型攻撃マルウェア検査サービス概要

専門アナリストによる脅威分析。対策や事後対応に関する提言。

「標的型攻撃マルウェア検査サービス」は、以下のプロセスで実施されます。必要に応じて調査状況を随時ご報告しながら、対策立案を支援します。

検査対象環境ヒアリング	検査対象ネットワークの環境をヒアリングさせて頂き、検査対象の端末数やエージェントの配布・実行方法などを検討。
エージェントのカスタマイズ	環境に応じてエージェントをカスタマイズ。パラメータのチューニング、および結果収集機能を環境に合わせて実装。
エージェントによるスキャン実施	エージェントを配布・実行し、各端末のHDDをスキャン。エージェントはインストールレス。実行ファイル起動でスキャン開始。
スキャン結果収集	疑陽性ファイル、検査ログファイルを収集。必要に応じて、該当端末にインストールされているソフトウェア情報をヒアリング。
スキャン結果概要分析	疑陽性ファイルを専門アナリストが概要分析。マルウェアの疑いがあるファイルを抽出し、概要分析結果を一次報告。
マルウェア解析	マルウェアの疑いがあるファイルを専門アナリストが詳細分析(リバースエンジニアリング)。マルウェアと判断された場合、そのエビデンスを抽出。
脅威分析	マルウェアの詳細分析結果、およびネットワーク環境情報などから、情報漏洩の有無など実質的な被害を分析。
報告会	マルウェア解析結果、脅威分析結果を報告会にてご報告。対策や事後対応について意見交換を実施。

OS(32bit)	Windows XP : Home, Professional, Media Center, Tablet PC Windows Vista : Home Basic, Home Premium, Business, Enterprise, Ultimate Windows 7 : Starter, Home Premium, Professional, Enterprise, Ultimate Windows 8 : Core, Pro, Enterprise Windows 8.1 : Core, Pro, Enterprise Windows 10 : Home, Pro, Enterprise, Education Windows Server 2003 : Standard, Enterprise, Datacenter Windows Server 2003 R2 : Standard, Enterprise, Datacenter Windows Server 2008 : Standard, Enterprise, Datacenter
OS(64bit)	Windows 7 : Starter, Home Premium, Professional, Enterprise, Ultimate Windows 8 : Core, Pro, Enterprise Windows 8.1 : Core, Pro, Enterprise Windows 10 : Home, Pro, Enterprise, Education Windows Server 2008 : Standard, Enterprise, Datacenter Windows Server 2008 R2 : Standard, Enterprise, Datacenter Windows Server 2012 : Foundation, Essentials, Standard, Datacenter Windows Server 2012 R2 : Foundation, Essentials, Standard, Datacenter
HDD	200MB以上の空き容量（検査対象端末）

※ 上記以外のWindows環境では動作確認を行っておりませんのでお問い合わせ下さい。
※ 検査を実施するためには、検査対象端末のHDDの空き容量が200MB以上である必要があります。
※ スキャン速度は、500ファイル/分が目安となりますが、環境により実際の速度は前後します。
※ ユーザー権限で実行された場合、ユーザー権限で開くことができないフォルダにつきましては検査対象外となりますので、管理者権限での検査を推奨いたします。

製品・サービスについてのお問い合わせは

株式会社ＦＦＲＩ
〒150-0013
東京都渋谷区恵比寿1-18-18 東急不動産恵比寿ビル4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/

2017年8月現在 Ver 2.00.09