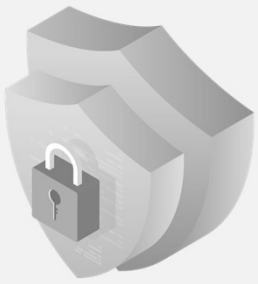
専門家向けツール
オブジェクト解析　Dr.Web vxCube
インシデント調査　Dr.Web FixIt!

不審なオブジェクトを解析するサンドボックス型インタラクティブアナライザー
Dr.Web vxCube

どのような機能か？
- 実際のユーザーのコンピュータを模倣した隔離環境でマルウェアサンプルを解析します。
- クラウドまたはローカルサーバー上で動作します。
- WebインターフェースまたはHTTP API経由で管理されます。



活用いただけるお客様
- なんらかのアンチウイルスを導入している企業
- マルウェア駆除サービスを提供するサービス企業
- サイバーインシデントを調査する情報セキュリティ部門
- 学生向けに実技授業を行う IT 系の大学/専門学校

サービス内容
- 解析されたファイルの悪意レベルを評価します。
- 検出されたファイルの挙動一覧を含む、詳細な解析レポートを提供します。
- テスト環境に接続して解析プロセスに関与することができます。
- システムへの侵入の痕跡（またはその兆候）をマシンリーダブル（機械可読）な形式で表示します。
- 修復ユーティリティをビルドします。
- 解析アーティファクト（サンドボックス内で解析されたサンプルが生成したオブジェクト）内での脅威を検出します。

次ページへ

専門家向けツール

インシデント調査の新たなソリューション

Dr.Web FixIt!

情報インフラへの不正侵入、既に実行された攻撃の足跡、
現在実行中の攻撃を検知し、システムを修復。

サービス内容
- システム検査
- 収集されたデータの解析
- 修復

システム検査　データを収集しレポートの作成
- インストールされたプログラムおよびアップデート
- 起動中のプロセス、または既に起動されたプロセス
- レジストリに書き込まれた不審なエントリの有無、
  そのエントリと他のオブジェクトとの関係
- インストールされたドライバー、ブラウザ拡張
- プロセス上にダウンロードされたモジュール
- システムログ
- ブートキットに隠されたものを含むディスクのセクター

収集されたレポート（データ）の解析
- システム検査で作成されたレポートを、アップロード
- スペシャリストによる解析
- フィルター機能により、以前までのレポートと比較処理を行う

修復
- 対象の悪意あるオブジェクトに対する処理に応じたビルドの作成
- インシデントによる影響が完全に修復するまで
  システムの検査を繰り返し実施

**Dr.Web FixIt! により
収集されたデータの解析**

感染の修復

**発生する可能性のある
損失の推定**

サイバー攻撃防止とともに、損失の減少を図るセキュリティ対策の策定

Doctor Web
©2003 -2024

株式会社Doctor Web Pacific　〒105-0003　東京都港区西新橋1-14-10 西新橋スタービル2F
TEL 03-6550-8770