

Dr.Web vxCube

www.drweb.co.jp

DEFEND WHAT YOU CREATE

- 不審なオブジェクトを解析する
インタラクティブなクラウド型
インテリジェントアナライザー
- 情報セキュリティエキスパート、
サイバー犯罪捜査官向け

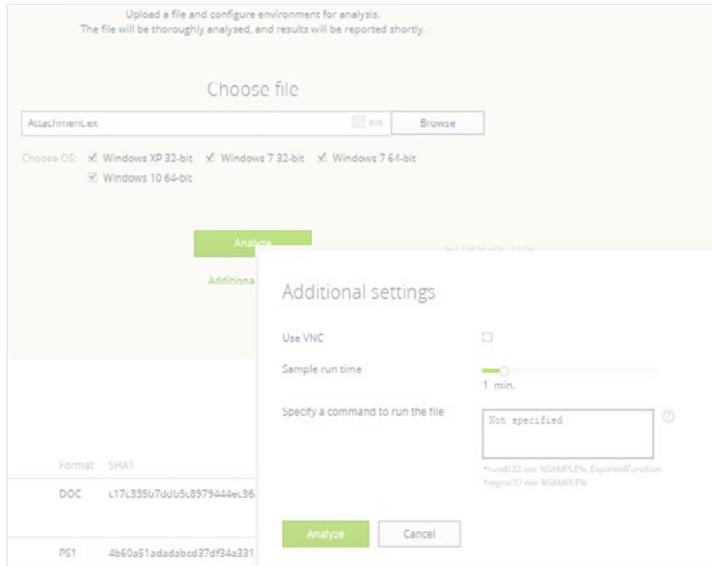


不審なオブジェクトを解析するインタラクティブなクラウド型インテリジェントアナライザーDr.Web vxCubeについて、案内します。Dr.Web vxCubeの機能は下記となります。

- 不審なファイルの悪意性の有無をオンラインでスキャンし確認します
- 必要なエビデンスが含まれるレポートを作成します。
- SOC/SIEMにデータを送信します。

ブラウザさえあれば、Dr.Web vxCubeサービスにアクセスし、不審なオブジェクトの解析ができます。

VNC (Virtual Network Computing)経由でDr.Web vxCubeへの接続が可能なことにより、ユーザーはリモートから解析過程に参加することができます。



オブジェクトが明らかに危険なものであると判定された場合、ご利用のシステムを修復するため、システムにインストール済みのアンチウイルスソリューションが対応する前に、Dr.Web CureIt! の特別なビルドが即座にユーザーへ提供されます。インストールが不要なDr.Web CureIt!は、他社アンチウイルスがインストールされたシステム上でも、動作するユーティリティです。

Dr.Web vxCubeの特徴

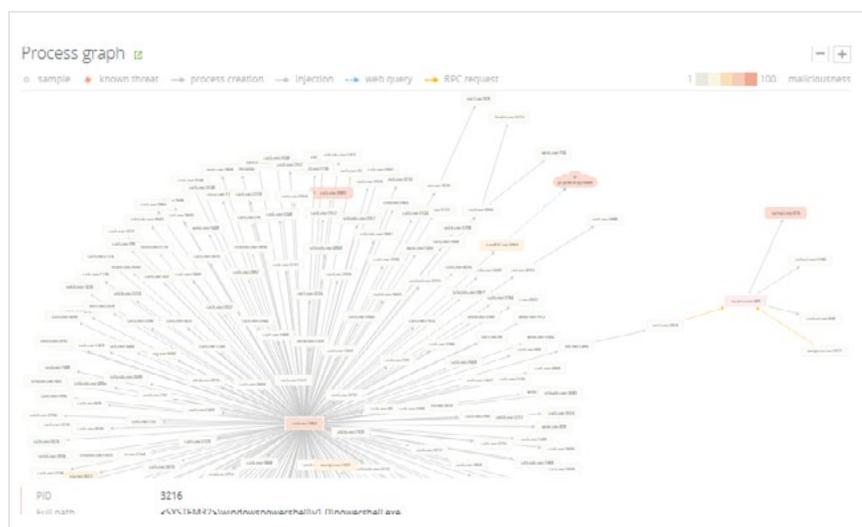
- ユーザー環境にマッチした環境下でのオブジェクト解析を実施
- 解析過程をモニター可能
- 解析のために不審なオブジェクトの挙動を再現
- 必要なデータが含まれるレポートを提供
- 正規ソフトウェアに埋め込まれる可能性のあるバックドアの有無を解析
- 悪意のあるコードのダウンロードを検出
- SOC および SIEM向けにデータのエクスポートを実施

さらに、Dr.Web vxCubeを用いると次のことが可能となります

- ゼロデイ脅威(0-hour threat)が実際に活動を開始する前に、その脅威がご利用のPC上にもたらすダメージとしてどのようなことが起こり得るかを徹底的に検討します。
- 貴社に対し、攻撃が行われたという仮想的なシナリオを考え、このような攻撃により、発生する被害の規模を事前に想定できます。
- 貴社ネットワークを標的にする犯罪者の狙いを徹底的に解析することができます。

本サービスを使うユーザーにとってのメリット

- 解析対象ファイルが挙動する仮想マシンのデスクトップ記録
- 悪意性レベルの評価
- Dr.Web CureIt! の特別なビルドの提供
- 解析されるファイルのリソースとの連携
- システムへ施された改変のリスト(autorunへの書き込み、ファイルおよびネットワークに対し実行されたアクションなど)
- 作成されたファイル、RAM、ネットワークパケットのダンプ
- WinAPIのログ
- 解析されるファイルのチェックサム
- 必要なサービスとの連携が容易



Dr.Web vxCubeの詳細について、<https://www.drweb.co.jp/vxcube/?lng=ja> をご覧ください。

トライアル版の入手

- 無料スキャン可能なファイルの総数は、10ファイルが限度となります。有効期間は、10日となります。
- トライアルの問い合わせ:
<https://download.drweb.co.jp/vxcube>

ライセンス購入

- 購入の問い合わせは、下記のサポート用ページにあるフォーム経由で送信されます(件名“購入”)。
<https://support.drweb.co.jp>

Dr.Web vxCubeの利用は、[使用許諾](#)の内容に準拠するものであり、Doctor Webの承認を得ない場合、ユーザーがその責任を負うものとします。



© Doctor Web, 2003–2019

Doctor Webは、ロシアに本社を置く、『Dr.Webアンチウイルスソフトウェア』の開発者です。その製品の開発は1992年に始まりました。

3rd street Yamskogo polya 2-12 A, Moscow, Russia, 125040

Tel.: +7 (495) 789-45-87 Fax: +7 (495) 789-45-97

<https://free.drweb.com>

