Dr.WEB®
1992年から

Dr.Web vxCube

- 標的型攻撃に用いられる脅威を含む未知の脅威(0-DAY)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です。
- 解析直後に、修復ユーティリティのビルドを直ちに実行します。
- 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

Dr.Web vxCube

アンチウイルスを使用していても、ウイルスがネットワークに潜んでいるのではないかという懸念がある場合、不審なファイルをアンチウイルスラボに提供することが、適切な対処であると考えられます。

しかし、ウイルスアナリストが実施する作業に対して費用と時間がかかります。

しかし、脅威への迅速な対応が必要不可欠です。

このような場合には、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が役立ちます。

Dr.Web vxCubeはスキャン開始1分後に、ファイルの悪意の有無を明らかにした上で、ファイルが加えたシステムへの改変を修復するためのユーティリティをビルドします。

▪ クラウド形アナライザーで、インストールが不要です。	▪ 悪意のあるソフトウェアの挙動について、詳細な解析を行います。	▪ 読みやすいレポート	▪ 自動化およびサーバーとの連携のためにAPIが用いられます。

Dr.Web vxCubeサービスを用いると、ファイルの悪意の有無を明らかにするだけでなく、ローカルおよびネットワークリソースとの連携に関する報告や修復ユーティリティDr.Web CureIt!の特別なビルドを入手することができます。

ご利用のPCにトロイの木馬が仕掛けられた場合、一体どのようなリスクがあるのでしょうか? トロイの木馬が実際に侵入する前に、そのリスクを検討しましょう。	**例えば、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ましょう。こうした攻撃により、発生する被害はどのような規模になるのでしょうか?** 被害の規模を事前に想定しましょう。	**サイバー犯罪者はどのような目的で貴社ネットワークを標的にしたのでしょうか?** Dr.Web vxCubeを利用することで、犯罪者の狙いを徹底的に解析することができます。

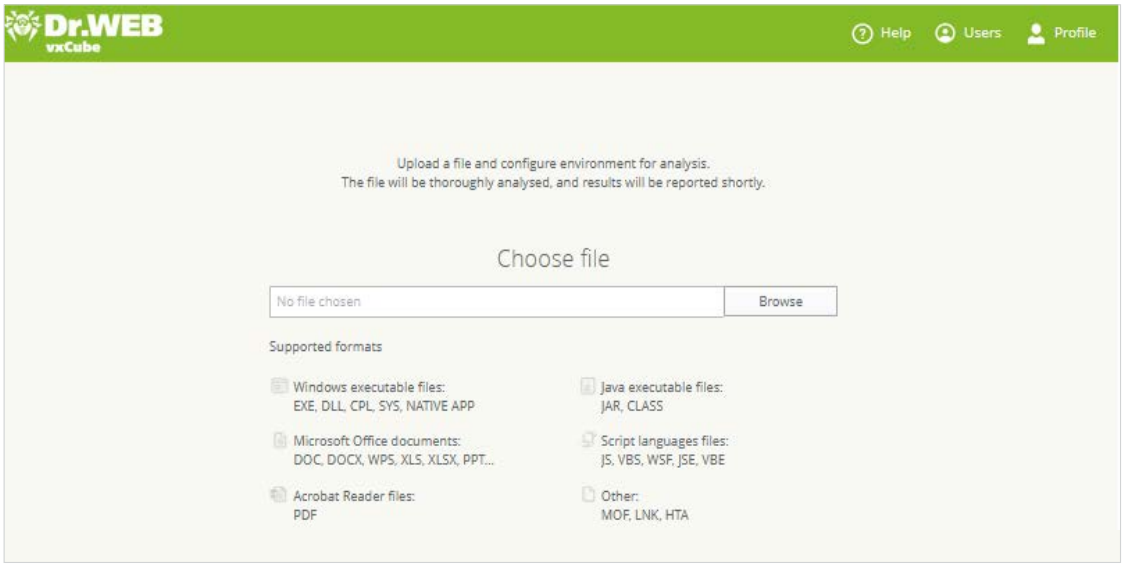
複数のOSに対応し、下記の犯罪者に一番よく狙われる一般的なアプリケーションを対象に解析が実行されます。

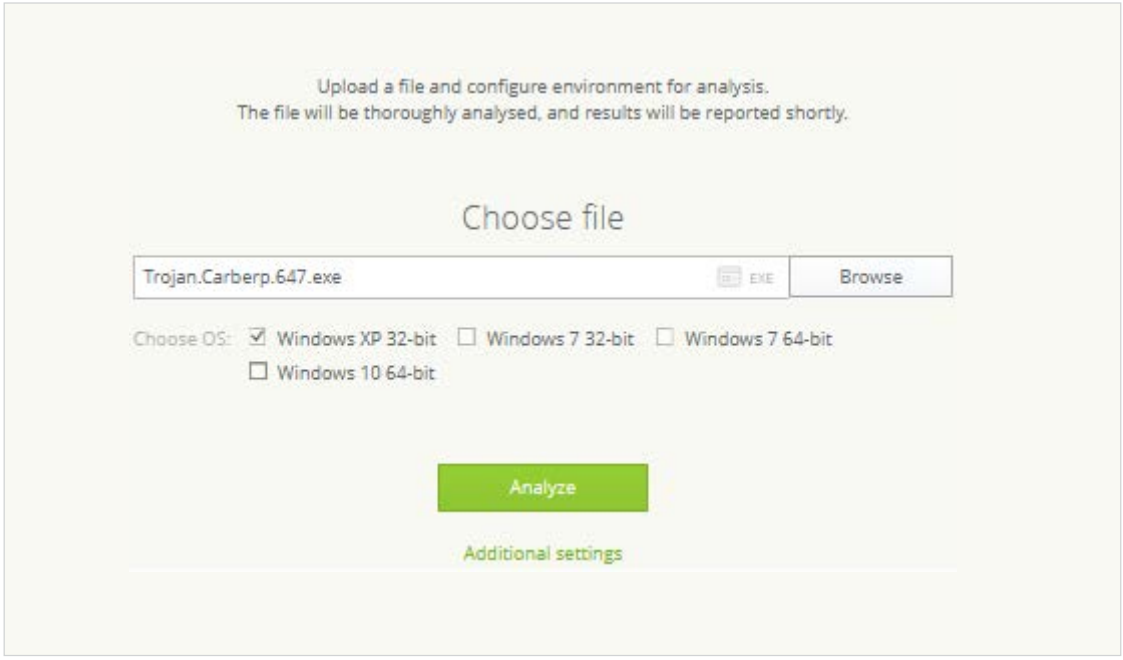
- Windows 実行ファイル
- Microsoft Office ドキュメント
- Acrobat Reader ファイル
- JAVA実行ファイル
- スクリプトファイル

! Dr.Web vxCubeサービスを企業と連携すると、スキャンされるファイル数を増やすだけでなく、標的型攻撃を含む最新の脅威を検出する確実性が高まります。不審なファイルのスキャンは、手動および自動モードの両方を利用できます 。

Dr.Web vxCubeサービス利用方法

1. ユーザーはクラウド型解析サービスへ不審なファイルを送信するために、必要なアクセスを取得します。
Dr.Web vxCube にアクセスし、利用するには、インターネット接続とブラウザーがあれば、十分です。





本サービスでは、Doctor Web個人情報保護方針https://company.drweb.co.jp/policy?lng=jaに基づき、個人情報の取り扱いを遵守します。Dr.Web vxCube経由で入手されたファイルと、他の経路で提供されたファイルは区別されます。

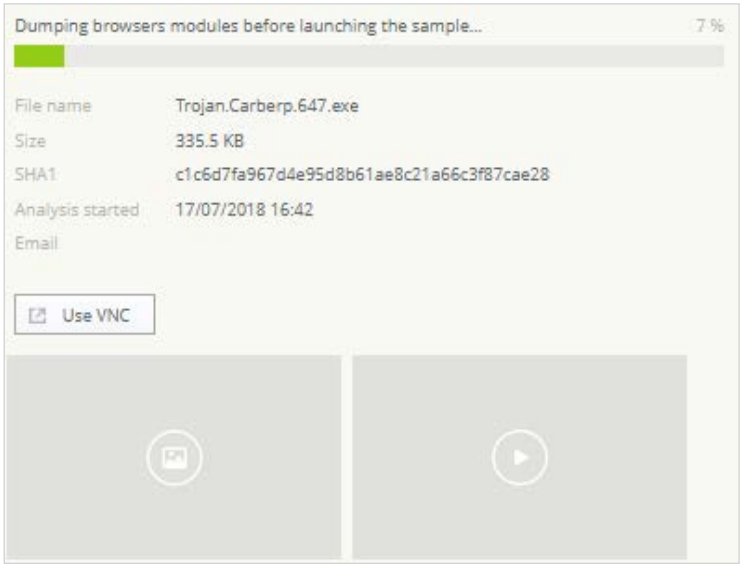
2. Dr.Web vxCubeは、独立した仮想環境の下で、ユーザーに送付された不審なオブジェクトの挙動の解析を自動的に行います。その際に、Doctor Webウイルスアナリストは参加しません。

スキャン時間は約1分です!

ユーザーは次の項目を指定できます。

- 解析対象となるアプリケーションのバージョンおよび対応OS
- 不審なファイルの挙動を徹底的に解析するのに1分で十分ではないと判断された場合には、任意のスキャン時間を設定で指定できます。
- VNC (Virtual Network Computing)経由でDr.Web vxCubeへの接続が可能であるため、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

! インタラクティブなモードで解析を管理するためには、ブラウザー設定にてポップアップウインドウの表示を許可する必要があります。



! マルウェアは専用のテスト環境下で自己を起動しようとする試みを監視することにより、自己の解析を防ごうとしています。そこで、Dr.Web vxCubeを作る過程において、マルウェアによる解析を防止する仮想マシンが開発されました。

3. 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、解析対象となったファイルの行動からシステムを修復するために、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。

利用されているアンチウイルスの更新のリリースを待たずに、最新の脅威を迅速に駆除することができます。

インストールが不要なDr.Web CureIt!は、他社アンチウイルス(Dr.Webではないアンチウイルス)を利用しているシステム上でも動作するユーティリティであるため、主たるアンチウイルスソリューションとしてDr.Webを利用されていない企業にとって、特に有用です。

4. 解析の完了後には、レポートが作成されます。レポートはDr.Web vxCubeお客様専用ページで閲覧するか、アーカイブ形式でダウンロードすることができます。本ページでは以前のスキャン結果レポートもご覧いただけます。

* ライセンスに含まれる場合

! スキャン結果のレポートには、解析されるプログラムに関するデータ(そのプログラムのコードの一部)が含まれるため、コンピュータにとって全く無害なものではありますが、マルウェアとして検知される可能性があります。

Dr.Web vxCube レポート

下記の内容にて、最終的なレポートは本サービスのユーザーに提供されます。

悪意性の判断

本サービスでは、マルウェアの悪意性が確認されます。

ネットワーク活動マップ

マルウェアが何処の国のサーバーにクエリしたかが明らかになります。

動画記録

ファイルの起動とその行動の過程を記録します。

動画記録

どのようなファイルをリクエストしたか、どのようなレジストリブランチに書き込みを実行したか、そして、アクセスがあったインターネットリソース等についての詳細な情報をご覧いただけます。

テクニカルな情報

システムにおける削除すべきコンポーネントとより強固なセキュリティを必要とするコンポーネントについて、アドバイスします。

作成されたファイル

解析されるサンプルが作成したファイル一覧とそのチェックサムが掲載されます。このデータを用いると、感染の修復を行えます。

APIログ

マルウェアがシステムの何処に潜んでいるかを明らかにします。

! Dr.Web vxCube使用許諾の6条に従い、商業的な目的を含め、レポートの公表については、Doctor Webより承諾を得なければなりません。

お役立ちリンク

トライアル版の入手: https://download.drweb.co.jp/vxcube?lng=ja
ライセンス: https://www.drweb.co.jp/vxcube/licensing?lng=ja

Doctor Webアンチウイルスラボスペシャリストによる悪意のあるファイルの解析

Dr.Web vxCubeによる解析結果で、ファイルの悪意性について確実性が低いと判断され、ユーザーはこうした判断について疑問を感じた場合には、ウイルス解析の豊富な経験を持つDoctor Webアンチウイルスラボのスペシャリストに解析を依頼することが可能です。

その困難さを問わず悪意のあるファイルを解析し、下記の内容にてレポートを提供いたします。

- マルウェアとそのモジュールの挙動パターンの解説
- オブジェクトをカテゴリで区別(確実に悪意性がある、悪意性の可能性がある等)
- ネットワークプロトコルの解析、コマンドサーバーの特定
- 感染したシステムへの影響および感染対策に関するアドバイス

アンチウイルス調査依頼について、以下のアドレスにお問い合わせください。: https://support.drweb.co.jp/support_wizard/?lng=ja

ウイルス関連インシデント (VCI) の調査

貴社はマルウェアで被害を受け、ウイルスアナリストによる調査が必要な場合、Doctor Webは、ウイルス関連のコンピュータインシデントに対する有料の調査サービスを提供しています。

調査サービス

- インシデントを解決するための初期アセスメント、調査範囲、必要な措置。
- VCIに関連している可能性のあるコンピュータやその他の項目(ハードディスク、テキスト、オーディオ、写真、動画)の調査。
- 特徴!「顧客に対する違法行為に関与/支援/隠匿/補助する可能性のある共犯者(包括的なリスクアセスメント)」や「不作為または義務の怠慢の例」を特定するための個人(社員)の心理的評価。
- VCIを防止するため、またはVCIを最小限に抑えられるようにするためのウイルス対策ソリューションの導入に関する推奨事項。

お役立ちリンク

ウイルス関連インシデント (VCI) の調査 : https://antifraud.drweb.co.jp/expertise?lng=ja
調査依頼: https://antifraud.drweb.co.jp/expertise?lng=ja

Doctor Webについて

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』のデベロッパーです。その製品の開発は1992年に始まりました。Doctor Webは、あらゆるビジネスにとって重要かつ不可欠な要素—情報セキュリティ—を満たすためのソフトウェアの、ロシア市場におけるキープレーヤーです。

Doctor Webはロシア市場においてアンチウイルスサービスを提供する初のベンダーとなり、現在においても、ロシア市場におけるインターネットサービスプロバイダ(ISP)に対するインターネットセキュリティサービスの第一人者として不動の地位を保っています。

Dr.Web のグローバルカスタマー

私達のカスタマーは世界各地のホームユーザーおよび大企業や中小企業、グローバル企業にまで及んでいます。Doctor Webの世界中に広がる多くのユーザーが、有能なロシアのプログラマーチームによって生み出される製品の品質の高さを明確に物語っています。

以下のページにてDr.Web カスタマーの一部をご確認いただけます。https://customers.drweb.co.jp/

Dr.Webの強みは何？

Dr.Web テクノロジーについて、Doctor Webが全ての権利を保有します。

Doctor Webはマルウェアを検出し修復する独自のテクノロジー、また自社のウイルスモニタリングサービス、アンチウイルスラボラトリーおよびテクニカルサポートサービスを有する世界でも数少ないアンチウイルスベンダーの一つです。

Doctor Web
2003–2018

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Tel.: +7 (495) 789–45–87
Fax: +7 (495) 789–45–97

https://www.drweb.com | https://free.drweb.com | https://ru.av-desk.com | https://curenet.drweb.com