Dr.WEB®
dal 1992

Dr.Web vxCube

- ANALIZZATORE CLOUD INTERATTIVO DI MINACCE SCONOSCIUTE (0-DAY), COMPRESE QUELLE UTILIZZATE PER ATTACCHI MIRATI
- CREAZIONE IMMEDIATA DELL'UTILITY DI CURA SULLA BASE DEI RISULTATI DELL'ANALISI
- PER I PROFESSIONISTI DELLA SICUREZZA INFORMATICA E I CYBER-CRIMINALISTI

Dr.Web vxCube

Immaginate che nonostante la protezione della rete tramite un antivirus, un file malevolo è riuscito ad infiltrarsi all'interno del perimetro. O avete dei giustificati sospetti che nella rete si trovi un "alieno".

Sarà una buona pratica inviare il file sospetto per l'analisi al laboratorio antivirus e attendere il verdetto. Ma il lavoro personalizzato degli analisti costa molto e talvolta richiede parecchio tempo.

Mentre il tempo stringe: la minaccia deve essere eliminata immediatamente.

In queste situazioni diventa uno strumento indispensabile l'analizzatore interattivo basato su cloud Dr.Web vxCube.

Entro un **minuto** Dr.Web vxCube valuterà quanto malevolo è un file e creerà un'utility di cura per eliminare le conseguenze del suo funzionamento.

▪ Non richiede installazione. Funziona nel cloud	▪ Completa analisi del comportamento del software malevolo	▪ Report comprensibili	▪ API per l'automazione dell'utilizzo del servizio

Dr.Web vxCube — strumento innovativo per combattere le ultime minacce sconosciute

Oggi la creazione di virus è un impresa criminale ben organizzata. I nuovi programmi malevoli, la maggior parte di cui è trojan, compaiono ogni giorno a centinaia di migliaia. Non tutti i campioni pervenuti per l'analisi al laboratorio antivirus Doctor Web sono programmi malevoli. Tuttavia, tutti devono essere elaborati dai nostri specialisti. Analizzare file malevoli richiede tempo, così come del tempo viene speso per assemblare e testare gli aggiornamenti, collocarli sui server di aggiornamento, installare gli aggiornamenti sui computer degli utenti.

L'obiettivo dell'antivirus è quello di prevenire l'infezione.

Si ritiene generalmente che un antivirus debba rilevare tutti i programmi malevoli al momento della loro infiltrazione nel computer. Tuttavia, gli autori di virus testano per il rilevamento da tutti gli antivirus i virus tecnologicamente complessi e particolarmente pericolosi, creati per ricavare profitti, prima di rilasciarli in "natura selvatica", affinché il virus possa esistere inosservato dagli antivirus quanto più a lungo possibile. Pertanto, intercorre sempre un intervallo di tempo tra il rilascio di un trojan dai malintenzionati e il momento in cui un suo campione viene analizzato nel laboratorio dei virus e viene creato l'antidoto.

C'è SEMPRE il rischio di infezione da un virus più recente SCONOSCIUTO.

Utilizzando il servizio Dr.Web vxCube, è possibile verificare un file e convincersi che è malevolo, identificare i suoi accessi a risorse locali e di rete, nonché ottenere una build speciale dell'utility di cura Dr.Web CureIt!.

Che disastro può combinare un trojan sul PC? Lo vedrete ancora prima che esso inizi ad agire.	**Quali possono essere le conseguenze di un ipotetico attacco alla vostra azienda?** Scopritelo in anticipo.	**Che cosa esattamente volevano fare i malintenzionati nella vostra rete?** Dr.Web vxCube lo esaminerà a fondo.

L'analisi viene eseguita in diversi sistemi operativi, vengono utilizzate le applicazioni tipiche, che sono oggi più frequentemente attaccate dai malintenzionati:

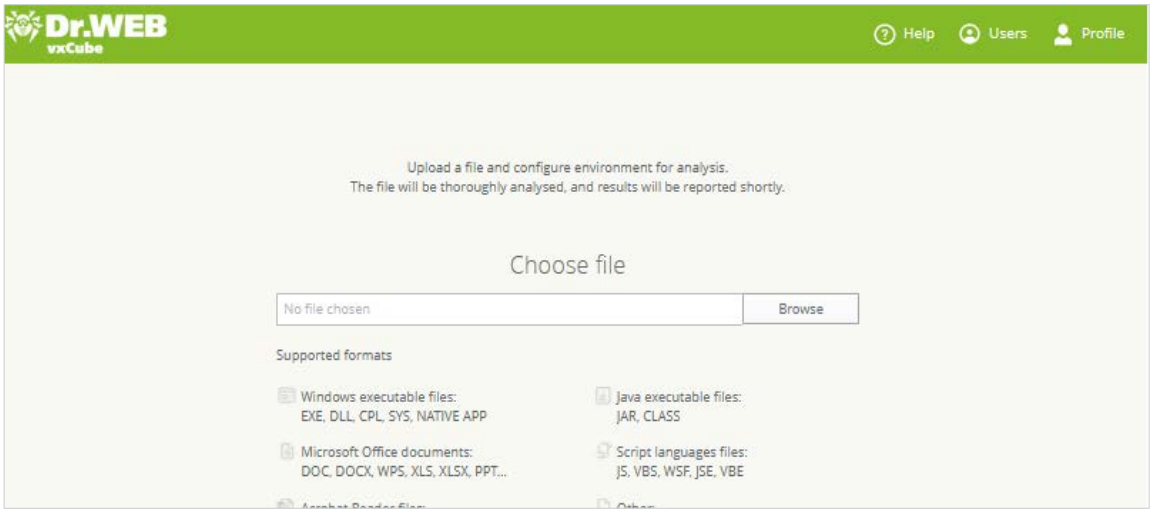
- File eseguibili di Windows
- Documenti Microsoft Office
- File Acrobat Reader
- File eseguibili JAVA
- File di script

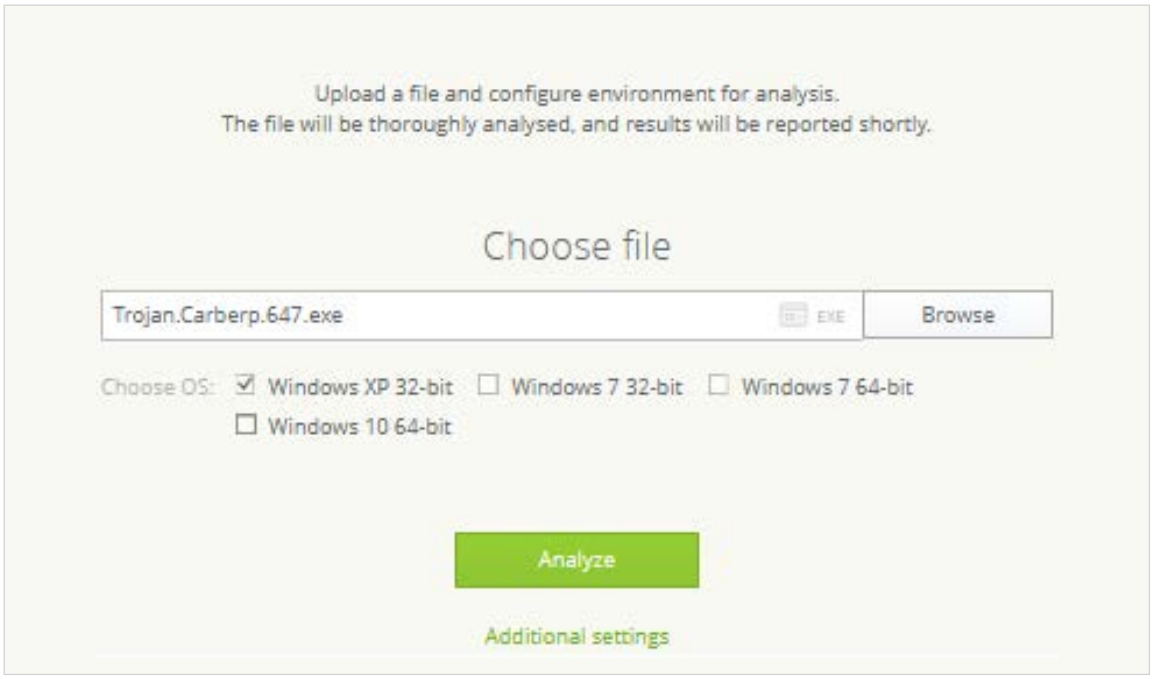
! La verifica di un file sospetto può essere eseguita sia in modalità manuale che automatica. L'integrazione di Dr.Web vxCube in servizi aziendali permette non solo di aumentare il numero di file controllati, ma anche di rilevare con un elevato grado di precisione gli attacchi più nuovi, tra cui gli attacchi mirati.

Come funziona Dr.Web vxCube

1. L'utente ottiene l'accesso all'analizzatore per inviare file sospetti per un'analisi basata su cloud.

Per accedere a Dr.Web vxCube e utilizzarlo, è sufficiente avere un browser e una connessione internet.





Il servizio rispetta i dati personali e confidenziali in conformità ai principi stabiliti nell'informativa sulla privacy Doctor Web: https://company.drweb.com/policy. I file arrivati per l'analisi attraverso Dr.Web vxCube sono separati da file che sono arrivati in altri modi.

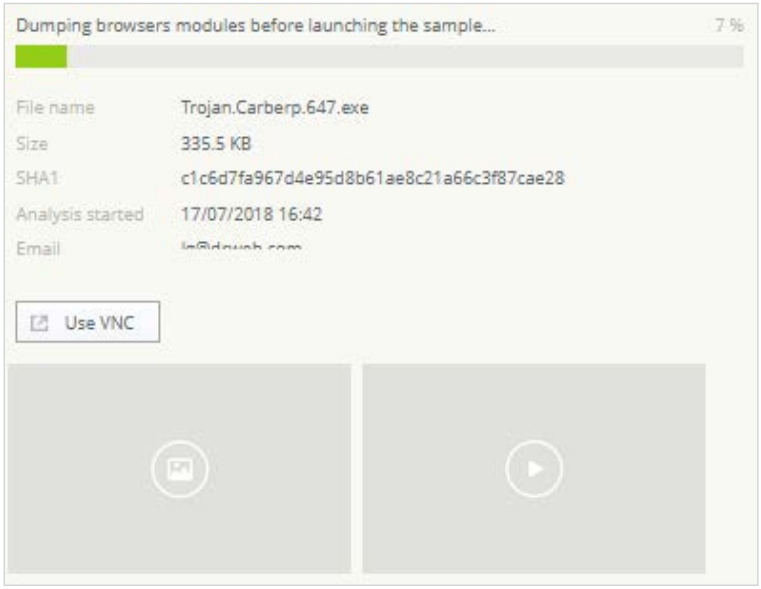
2. L'analizzatore esegue in un ambiente isolato un oggetto inviato dal ricercatore e ne studia il comportamento. L'analisi viene eseguita automaticamente, senza partecipazione degli analisti di virus Doctor Web.

La durata della verifica è a partire da un minuto!

Il ricercatore può:

- specificare in quali sistemi operativi e con quali versioni di applicazioni deve essere eseguita la verifica;
- definire nelle impostazioni il tempo di verifica desiderato, se il ricercatore ritiene che un minuto non sia sufficiente per un'analisi completa di un file sospetto;
- osservare — in remoto attraverso l'interfaccia di Dr.Web vxCube — l'avanzamento dell'analisi e persino influenzare il corso di analisi connettendosi all'analizzatore tramite VNC (Virtual Network Computing) per partecipare al processo di ricerca.

! Per gestire il processo di analisi in modalità interattiva, nel browser deve essere consentita l'apertura di finestre pop-up.



! Come è noto, i programmi malevoli monitorano i tentativi del proprio avvio in un ambiente di test specifico ed ostacolano la propria analisi. Nel processo di sviluppo del servizio Dr.Web vxCube è stata creata una macchina virtuale protetta dall'analisi da parte dei programmi malevoli.

3. **Se un oggetto rappresenta chiaramente una minaccia, l'utente riceve subito una build speciale dell'utility di cura Dr.Web CureIt!* per ripulire il sistema dalle azioni eseguite dal file analizzato.**

Questo permette di neutralizzare il più rapidamente possibile una minaccia più recente senza aspettare gli aggiornamenti dell'antivirus in uso.

Grazie all'universalità dell'utility Dr.Web CureIt! che è in grado di funzionare senza installazione in qualsiasi sistema in cui viene utilizzato un altro antivirus (diverso da Dr.Web), questo sarà particolarmente utile per le aziende che non ancora utilizzano Dr.Web come il software di protezione principale.

4. **Sulla base dei risultati dell'analisi viene fornito un report. Può essere visualizzato nell'area personale dell'utente di Dr.Web vxCube o scaricato come archivio. Inoltre, nell'area personale possono essere visualizzati i risultati delle verifiche precedenti.**

* Se tale opzione è inclusa nella licenza.

! Il report sui risultati della verifica contiene dati sul programma analizzato, in particolare, porzioni del suo codice, per cui può essere identificato come un programma malevolo, ma senza rappresentare alcun pericolo per il computer.

Report del servizio Dr.Web vxCube

Il report finale fornisce all'utente del servizio le seguenti informazioni.

Valutazione delle caratteristiche malevole

Il servizio valuta se il programma analizzato è malevolo, nonché quanto può essere pericoloso.

Una mappa dell'attività di rete

Indica a server in quali paesi del mondo si connetteva il programma malevolo.

Registrazione video

Visualizará el proceso de inicio y funcionamiento del archivo.

Relazioni

Mostra a quali file accedeva il programma, in quali rami del registro effettuava registrazioni, quali risorse Internet venivano utilizzate ecc.

Informazioni tecniche

Suggeriscono che cosa eliminare dal sistema, alla protezione dei quali sue parti prestare maggiore attenzione.

File creati

Viene riportato l'elenco dei file creati dal campione analizzato con i relativi checksum. Conoscendo questi file, sarà possibile eliminare le conseguenze dell'infezione.

Log API

Mostrerà in che modo il programma malevolo si nasconde nel sistema.

! Secondo il paragrafo 6 del Contratto di licenza per Dr.Web vxCube, la pubblicazione o un'altra distribuzione dei report, tra le altre cose anche a fini di lucro, deve essere concordata per iscritto con Doctor Web.

Link utili

Accesso di prova: https://download.drweb.com/vxcube

Licenze: https://www.drweb.com/vxcube/licensing

Analisi di file malevoli da parte di esperti del laboratorio antivirus Doctor Web

Nessun servizio automatizzato potrà mai sostituire l'esperienza e le conoscenze di un analista di virus. Nel caso in cui il verdetto Dr.Web vxCube non riconosce un file analizzato come univocamente malevolo, ma avete ancora dei dubbi su questa decisione, vi offriamo di usufruire dei servizi di esperti del laboratorio antivirus Doctor Web che hanno molti anni di esperienza nell'analisi dei virus.

I servizi includono l'analisi di file malevoli di qualsiasi complessità, in base ai risultati della quale viene elaborato un resoconto contenente:

- la descrizione degli algoritmi di funzionamento del software malevolo, nonché dei suoi moduli;
- la categorizzazione di oggetti: univocamente malevolo, potenzialmente malevolo (sospetto), ecc.;
- l'analisi del protocollo di rete e l'identificazione dei server di comando;
- l'influenza sul sistema infetto e le raccomandazioni per l'eliminazione dell'infezione.

Le richieste di ricerca antivirus si accettano sull'indirizzo: https://support.drweb.com.

Perizia di incidenti informatici legati ai virus

Se la vostra azienda è rimasta vittima dell'attività di un software malevolo e vi serve una perizia qualificata di quanto accaduto effettuata da parte di analisti di virus, usufruite dei servizi di un reparto speciale dell'azienda Doctor Web.

La perizia degli incidenti informatici legati a virus include:

- Valutazione preliminare dell'incidente, del volume della perizia e delle misure necessarie per eliminare le conseguenze di quanto accaduto.
- Studi dagli esperti di artefatti informatici e altri (dischi rigidi, materiali testuali, audio, foto, video) che presumibilmente riguardano l'incidente informatico legato a virus.
- Senza pari! Perizia psicologica degli individui (del personale) al fine di rivelare i fatti di coinvolgimento negli atti illeciti contro il cliente / nella relativa complicità / favoreggiamento / incoraggiamento (identificazione completa dei rischi), e inoltre i fatti di inazione o trascuratezza dei doveri d'ufficio.
- Raccomandazioni sulla costruzione di un sistema di protezione antivirus al fine di prevenire incidenti informatici legati a virus o ridurne il numero in futuro.

Link utili

Sulla perizia degli incidenti informatici legati a virus: https://antifraud.drweb.com/expertise

Richiesta di perizia: https://support.drweb.ru/expertise

L'azienda Doctor Web

Doctor Web — fornitore russo di software antivirus di protezione delle informazioni sotto il marchio Dr.Web. I prodotti Dr.Web vengono sviluppati fin dal 1992. L'azienda è un attore chiave nel mercato russo dei software studiati per soddisfare un'esigenza essenziale delle aziende — quella di sicurezza delle informazioni.

Doctor Web è stata la prima azienda ad offrire sul mercato russo il modello innovativo di utilizzo dell'antivirus come servizio e fino ad oggi rimane leader indiscusso del mercato russo dei servizi internet di sicurezza per i fornitori di servizi informatici.

Si fidano di Dr.Web

Grazie alla presenza nell'organico Doctor Web di esperti di varie problematiche di sicurezza delle informazioni, l'azienda può tenere conto, al livello massimo, delle particolarità di lavoro di aziende di varie dimensioni e con diversi profili di attività e offrire ai clienti la migliore scelta di prodotti di qualità con un costo totale minimo.

Tra i consumatori dei prodotti Dr.Web ci sono utenti privati da tutte le regioni del mondo e grandi imprese russe, piccole organizzazioni e aziende della spina dorsale. La geografia degli utenti di Dr.Web testimonia l'alta fiducia nel prodotto creato da programmatori russi di talento.

Ecco solo alcuni clienti di Dr.Web: https://customers.drweb.com.

Perché Dr.Web?

Tutti i diritti sulle tecnologie Dr.Web appartengono all'azienda Doctor Web. L'azienda è uno dei pochi fornitori di antivirus al mondo che possiedono le proprie tecnologie uniche di rilevamento e neutralizzazione di programmi malevoli; ha il proprio laboratorio antivirus, un servizio di monitoraggio dei virus globale e un servizio di supporto tecnico.

Russia, 125124, Mosca, la 3° via Yamskogo polya, 2-12A
Tel.: +7 (495) 789–45–87
Fax: +7 (495) 789–45–97
Website: www.drweb.com
Email: pr@drweb.com

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