Dr.WEB®
dal 1992

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks*

* Distrugge minacce attive e attacchi nuovi

© Doctor Web, 2021

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks

Un antivirus non basato su firme antivirali di nuova generazione rafforza la protezione del PC «in collaborazione» con un antivirus tradizionale

Per qualsiasi azienda sono critici le violazioni dei processi business, gli accessi non autorizzati ai dispositivi, lo sfruttamento delle vulnerabilità, il password cracking, il phishing e altre attività illegali che vengono effettuate tra le altre cose anche nel corso di incidenti informatici legati a virus tramite software malevoli.

Purtroppo, oggi per una serie di motivi non si può fare affidamento sulla protezione antivirus di un solo fornitore.

Gli autori di virus testano i virus tecnologicamente complessi e particolarmente pericolosi per il rilevamento tramite i database dei virus di tutti gli antivirus, prima di rilasciare tale virus in «natura selvatica».

Pertanto, se si fa affidamento solo sulla verifica tramite i database dei virus di un antivirus — indipendentemente dalla loro qualità — i malintenzionati avranno sempre un vantaggio di tempo: un codice malevolo può già essere noto al fornitore di un antivirus, ma non è ancora stato ricevuto dall'antivirus sul dispositivo dell'utente.

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

Quando si ha bisogno di due antivirus?

- Quando l'antivirus principale salta minacce.
- Quando l'antivirus principale non può essere aggiornato frequentemente.
- Quando il PC per lungo tempo è fuori dalla zona di accesso a Internet.
- Quando il PC si trova in una rete isolata in cui gli aggiornamenti vengono consegnati raramente.

Un antivirus non basato su firme antivirali è sempre necessario: non potete sapere se il vostro antivirus ha già saltato un programma malevolo o meno.

Vi offriamo al fine di rafforzare la protezione della rete locale e di singoli computer dalle minacce malevole più recenti e particolarmente pericolose — compresi i trojan cryptolocker — di utilizzare in aggiunta a un antivirus tradizionale basato su firme (diverso da Dr.Web) l'antivirus non basato su firme **Dr.Web KATANA**.

Oggi nessun antivirus conosce il 100% dei programmi malevoli al momento dell'infiltrazione. Purtroppo, i programmi malevoli più pericolosi, quali i cryptolocker, possono raggirare i metodi di protezione antivirus tradizionali.

Anche se un antivirus in uso è capoclassifica di vari test, bisogna ricordare che al momento dei test tutti i programmi malevoli di test erano già conosciuti dagli analisti e organizzatori dei test. E quindi, il premio nei test non dice nulla sulla capacità di questo antivirus di respingere le minacce attive sconosciute al momento dell'attacco.

Perché molte aziende protette da prodotti vincitori dei test sono rimaste vittime di WannaCry? I loro antivirus non avevano la firma del nuovo trojan, e gli analizzatori comportamentali non sono riusciti a proteggerle.

Mentre i clienti di Dr.Web non sono stati colpiti da WannaCry.

Una protezione addizionale dalle moderne minacce più recenti, che possono essere non conosciute dal antivirus basato su firme antivirali in uso, può essere realizzata sulla base delle tecnologie di **Dr.Web KATANA** che analizzano il comportamento dei programmi cercando segni di comportamento malevolo nei processi in esecuzione. Il prodotto protegge dalle minacce che non vengono rilevate tramite i metodi di rilevamento tradizionali (basati su firme antivirali)..

Tutti i trojan lo fanno

Operano secondo gli algoritmi simili,	**Commettono lo stesso errore:**
utilizzano gli stessi punti critici nei sistemi operativi per infiltrarsi, hanno set di funzioni malevole uguali.	iniziano ad agire per primi (attaccano il sistema).

L'inizio della manifestazione dell'attività di un trojan è sufficiente affinché Dr.Web KATANA lo veda e lo disinneschi.

L'antivirus non basato su firme antivirali Dr.Web KATANA svolge gli stessi compiti di un antivirus tradizionale:

- riconosce i processi malevoli,
- respinge gli attacchi dei programmi malevoli,
- blocca i tentativi di infiltrazione nel sistema — ma lo fa... in modo più fine.

Dr.Web KATANA rileverà l'attività malevola non appena un trojan proverà ad agire.

- Molti trojan operano secondo gli algoritmi simili, utilizzano gli stessi punti critici nei sistemi operativi per infiltrarsi, hanno set di funzioni malevole uguali.
- Tutti i trojan commettono lo stesso errore: iniziano ad operare per primi (attaccano il sistema).
- Una manifestazione dell'attività di un trojan è sufficiente affinché Dr.Web KATANA veda il nemico e gli infligga il colpo mortale.
- Dr.Web KATANA analizza "al volo" il comportamento delle minacce e termina immediatamente gli script e i processi malevoli che l'antivirus in uso non è riuscito a riconoscere (= HA SALTATO).

E firme antivirali non sono necessarie, il che rende Dr.Web KATANA un'arma estremamente leggera.

Gli analizzatori comportamentali tradizionali si basano sulle regole di comportamento di software illegittimi conosciuti, le quali sono rigorosamente trascritte in una knowledge base.

Anche i malintenzionati conoscono queste regole!

La presenza di vulnerabilità e la possibilità di introdurre exploit consente loro di raggirare tale protezione.

Dr.Web KATANA agisce «al volo»	**L'analisi dura frazioni di secondo**	**Non sono necessari accessi ai database dei virus «pesanti»**

Che cosa viene controllato da Dr.Web KATANA

- Processi di applicazioni legittime.
- Le porzioni critiche del sistema e i servizi di sistema — aree di avvio del disco, chiavi del registro di sistema, comprese quelle responsabili dei driver di dispositivi virtuali.
- Regole di avvio dei programmi.
- Disattivazione della modalità provvisoria di Windows.
- Possibilità di aggiungere alle routine di base del sistema operativo nuovi task richiesti dai malintenzionati.
- Caricamento di driver nuovi o sconosciuti dall'utente.
- Comunicazione tra i componenti di un programma spione e il suo server di gestione.
- Processi di backup standard.
- Tutti i browser popolari (Internet Explorer, Mozilla Firefox, Yandex.Browser, Google Chrome, Vivaldi Browser).
- Le applicazioni MS Office (Word/Excel/InfoPath/Lync/Access/Outlook/Visio/WordPad), Windows Media Player.
- Le applicazioni di sistema.
- Le applicazioni che utilizzano le tecnologie java (Java 1.8/6/7), flash e pdf (Acrobat Reader)

Funzionalità di Dr.Web KATANA

- Protegge le aree critiche del sistema contro le modifiche da parte dei programmi malevoli.
- Rileva e termina gli script e processi malevoli, sospetti o inaffidabili.
- Riconosce le modifiche di file indesiderate, monitorando il funzionamento di tutti i processi nel sistema per scoprire le attività tipiche del comportamento dei programmi malevoli (per esempio azioni dei trojan ransomware), non permettendo agli oggetti malevoli di incorporarsi nei processi di altri programmi.
- Rileva e neutralizza le minacce più recenti: trojan ransomware (cryptolocker), web injector, oggetti malevoli gestiti da remoto (vengono propagati per organizzare botnet e spiare utenti), nonché packer di virus.
- Protegge dagli exploit — oggetti malevoli che cercano di sfruttare le vulnerabilità, comprese quelle non conosciute da nessuno tranne che dagli autori di virus (le cosiddette vulnerabilità "zero-day").
- Controlla il funzionamento non solo dei browser più popolari, ma anche di qualsiasi plugin; protegge dai programmi che bloccano browser.
- Blocca la possibilità di modifica dei settori di avvio del disco da parte dei programmi malevoli per rendere impossibile l'avvio (per esempio, dei trojan) sul computer.

- Previene la disattivazione della modalità provvisoria di Windows, bloccando modifiche del registro.
- Non permette ai programmi malevoli di aggiungere alle routine di base del sistema operativo nuovi task richiesti dai malintenzionati. Blocca determinate chiavi del registro di Windows, il che impedisce ai virus, per esempio di modificare l'aspetto normale del Desktop o di nascondere la presenza di un trojan nel sistema tramite un rootkit.
- Non permette ai programmi malevoli di modificare le regole di avvio dei software.
- Blocca il caricamento di driver nuovi o sconosciuti all'insaputa dell'utente.
- Blocca l'esecuzione automatica di programmi malevoli, nonché di determinate applicazioni, quali gli anti-antivirus, non permettendo che si iscrivano al registro per il successivo avvio automatico.
- Blocca i rami del registro responsabili dei driver di dispositivi virtuali, il che rende impossibile l'installazione di un nuovo dispositivo virtuale.
- Blocca la comunicazione tra i componenti di un programma spione e il server che li controlla.
- Non permette ai software malevoli di compromettere il normale funzionamento dei servizi di sistema, per esempio, interferire nella regolare creazione delle copie di backup dei file.

Algoritmo di funzionamento di Dr.Web KATANA

- Quando rileva un tentativo di sfruttamento di una vulnerabilità, Dr.Web termina forzatamente il processo del programma sotto attacco. L'antivirus non esegue alcun'azione sui file dell'applicazione, neanche lo spostamento in quarantena.
- Come informazione, l'utente vede un avviso di blocco di un tentativo di operazione malevola, che non richiede alcuna risposta.
- Nel log degli eventi Dr.Web viene creato un record di blocco di un attacco.
- La knowledge base cloud del sistema riceve un avviso immediato sull'incidente. Se necessario, gli specialisti Doctor Web risponderanno istantaneamente ad esso — per esempio, migliorando l'algoritmo di controllo.

Come Cloud Dr.Web aiuta a proteggere

Il Cloud Dr.Web contiene:

- dati sugli algoritmi dei programmi che hanno intenzioni malevole;
- informazioni sui file noti come "puliti";
- informazioni sulle firme digitali compromesse di noti produttori di software;
- informazioni sulle firme digitali dei software pubblicitari / potenzialmente pericolosi;
- algoritmi di protezione delle applicazioni.

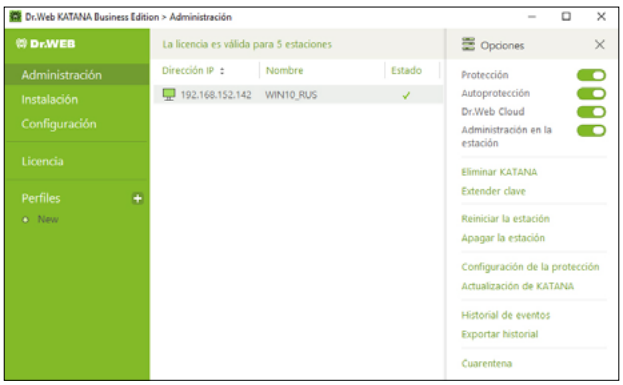
Il sistema cloud riceve informazioni sul funzionamento di Dr.Web KATANA sul PC protetto, comprese le informazioni sulle ultime minacce rilevate, il che permette di rispondere rapidamente a difetti identificati nel funzionamento del sistema e di aggiornare le regole conservate localmente sul computer.

Non avviene nessun trasferimento dei file dell'utente dal sistema protetto ai server Doctor Web!

Massima anticipazione	Resistenza eccezionale	Possibilità di funzionamento autonomo
▪ Dr.Web KATANA fornisce la protezione praticamente dal momento dell'avvio del sistema operativo. ▪ Inizia a proteggere ancora prima della fine dell'avvio dell'antivirus tradizionale basato su firme antivirali — del vostro altro antivirus!	▪ Dr.Web KATANA include un modulo di auto-protezione senza pari nel settore Dr.Web SelfPROtect. ▪ Se un trojan "ucciderà" il processo dell'altro antivirus, quindi dovrà disabilitare Dr.Web KATANA, ma verrà ostacolato dal modulo di auto-protezione. ▪ Grazie all'auto-protezione, Dr.Web KATANA reggerà e il processo malevolo verrà fermato.	▪ I trojan non sono in grado di diffondersi in autonomo. ▪ I dipendenti aziendali li portano su chiavette usb e altri dispositivi. ▪ Dove non è possibile installare un antivirus "pesante" basato su firme antivirali, darà una mano l'antivirus non basato su firme antivirali Dr.Web KATANA che ha requisiti di sistema minimi e può funzionare senza accesso a Internet.

Gestione

▪ Installazione centralizzata sulle postazioni protette della rete, impostazione e monitoraggio degli eventi di virus, nonché dello stato di Dr.Web KATANA sulle postazioni protette.	▪ Scenari di sicurezza predefiniti (ottimale, medio, paranoicale) — il prodotto funziona direttamente «out-of-the-box».	▪ Possibilità di creare regole flessibili per le applicazioni affidabili e di prevenire conflitti di software durante il funzionamento di Dr.Web KATANA.	▪ Possibilità di impostare i parametri di controllo sicurezza per un'applicazione specifica, fornendo per essa l'accesso solo a determinate risorse.

Pannello di controllo	Agent
	

Compatibilità

Nel corso dello sviluppo del software Dr.Web KATANA è stata confermata la compatibilità con i prodotti TrendMicro, Symantec, Kaspersky, Mcaffee, ESET e altri ancora.

Novità! Dr.Web vxCube

Analizzatore di oggetti sospetti basato su cloud intelligente interattivo per i professionisti della sicurezza informatica e i cyber-criminalisti.

Dr.Web vxCube:

- Analizza in remoto un oggetto in un ambiente che corrisponde proprio alla vostra situazione
- Permette di osservare il processo di analisi
- Riproduce qualsiasi azione dell'oggetto sospetto per esaminarla
- Fornisce un report completo dell'analisi fatta

Nel caso di rilevamento di una minaccia verrà creata una **build speciale dell'utility Dr.Web CureIt**! al fine di curare l'infezione del vostro sistema – prima ancora che il problema possa essere risolto dai vostri strumenti di protezione installati. Dr.Web CureIt! è in grado di funzionare senza installazione anche in presenza di un altro antivirus.

Maggiori informazioni su Dr.Web vxCube

Perizia di incidenti informatici legati ai virus

La perizia 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.

Per maggiori informazioni sulla perizia Doctor Web

Le richieste di perizia si accettano sull'indirizzo:

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.

© Doctor Web 2003–2021

2-12A, 3rd street Yamskogo polya,
Moscow, Russia, 125124

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

www.drweb.com