Dr.WEB®
dal 1992

Come scegliere l'antivirus

Metodica di scelta dei software di protezione antivirus

Ai proprietari di imprese, ai capi dei reparti IT delle aziende e organizzazioni, e inoltre agli specialisti nei sistemi di protezione antivirus aziendali

Dr.WEB®
dal 1992

SOMMARIO

Introduzione

Al momento sul mercato ci sono parecchie offerte di software antivirus. Uno penserebbe che sia facile scegliere la cosa migliore — tanto più che tra i leader dei test degli antivirus spesso ci sono persino soluzioni gratuite — un'ottima opportunità di risparmio! Magari le cose fossero così semplici...

- Buongiorno, abbiamo preso un cryptolocker, l'antivirus ... non ha aiutato.
- Buongiorno gentile team di Dr.Web, aiutate a decriptare un computer infettato dal virus WannaCry. L'infezione si è verificata all'apertura di siti (quale sito esattamente non ne ho idea perché non ho subito notato che si era verificata un'infezione), era installato l'antivirus ...

I puntini di sospensione nelle citazioni soprastanti sostituiscono i nomi degli antivirus di cui gli utenti si sono rivolti all'azienda Doctor Web per la decriptazione in seguito a un'infezione dal trojan WannaCry — un'epidemia che ha colpito persino le aziende più grandi.

Ci aggiungeremo che le descrizioni delle tecnologie impiegate da un antivirus per rilevare programmi malevoli assomigliano a degli incantesimi magici, e il problema di scelta di una soluzione che realmente protegge diventa davvero un problema.

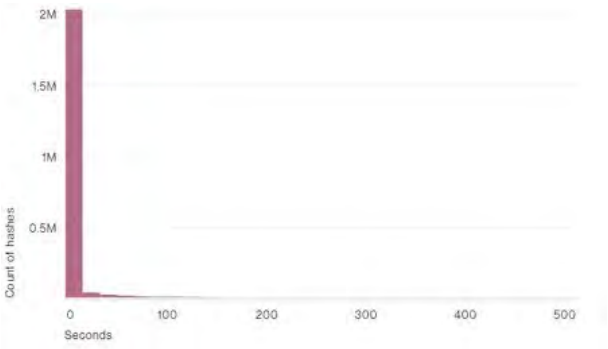
I. Principali cause di infezione e contromisure

Quasi ogni giorno nei mass media viene segnalata un'infezione di aziende e organizzazioni diverse. A volte vengono segnalati più milioni di perdite. La maggior parte di queste aziende utilizzava un antivirus al momento dell'infezione. Perché succede questo?

1. I malfattori hanno la possibilità di automatizzare lo sviluppo dei programmi malevoli, di conseguenza, il numero di campioni di malware che arrivano in un giorno per l'analisi nell'azienda Doctor Web raggiunge un milione!

- La necessità di aggiungere rapidamente nuove regole ai database antivirus, ai database delle regole del firewall e della protezione preventiva porta all'ingombramento della spazzatura, pertanto, l'azienda Doctor Web ripulisce regolarmente questi database dai record duplicati senza perdita di qualità del rilevamento.
- Una caratteristica unica dei database antivirus Dr.Web è un algoritmo di ricerca delle firme antivirali nei database antivirus, database delle regole del firewall e dell'analisi comportamentale, il quale non aumenta il tempo di ricerca con l'aumento del numero di record.

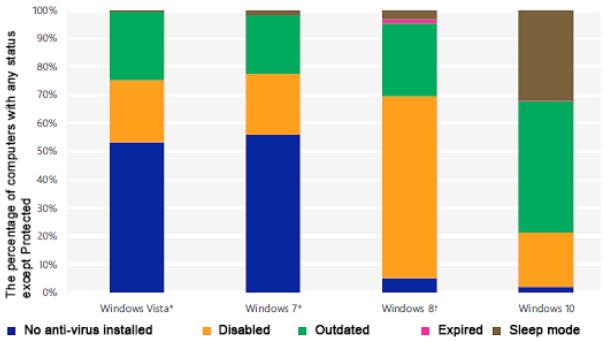
Un antivirus non dovrebbe rallentare!



Oltre il 99% dei campioni di programmi malevoli (hashes) "vive" 58 secondi e meno!

2. Gli utenti dei software antivirus non li aggiornano o addirittura li disattivano dopo l'installazione.

- Le statistiche scansione computer dall'utility di verifica di emergenza Dr.Web CureIt! mostrano che fino al 60% dei computer non è protetto in misura adeguata.
- Quasi il 30% degli utenti della versione gratuita dell'utility Dr.Web CureIt! utilizza l'antivirus incorporato nell'SO Windows 7 e 10 Microsoft Windows Defender.



Threat rating

Period: week; 10 lines

Name	Class	%
DFH:HOSTS.corrupted	virus	6.73
Program.MediaGet.142	riskware	2.54
Program.Unwanted.1183	riskware	2.21
Trojan.InstallCore.2896	virus	1.24
Program.Unwanted.276	riskware	1.17
Adware.Zaxar.62	adware	1.08
Program.Unwanted.2	riskware	1.02
Program.Unwanted.1678	riskware	0.86
Program.Zona.86	riskware	0.75
Adware.Elemental.1	adware	0.69

Total number: 524508

Statistiche scansione computer dall'utility Dr.Web CureIt!

Dr.Web trova minacce!

3. Gli utenti dei software antivirus ignorano gli avvisi del sistema di protezione, lo configurano in modo che i file malevoli arrivando nel sistema non vengono controllati dall'antivirus. ▪ Una delle cause principali di infezione computer è l'esclusione dalla scansione antivirus da parte dell'utente dei programmi che hanno l'accesso a Internet e di interi dischi del computer. ▪ Un altro metodo per abbassare il livello di protezione dell'antivirus è abbassare il livello di protezione del componente Protezione preventiva.	**! La maggior parte delle infezioni avviene a seguito delle azioni dei dipendenti aziendali, dei loro clienti o partner.**
4. Nelle reti locali non vengono installati per lungo tempo gli aggiornamenti ed è consentito l'uso di servizi vulnerabili. ▪ Gli exploit attraverso cui avviene un'intrusione in un sistema attaccato sono progettati per le vulnerabilità rilevate fino a tre anni fa e più! Effettivamente, il tempo di disponibilità di una falla coincide con il tempo di vita di un sistema operativo! ▪ Il cryptolocker WannaCry si è diffuso attraverso un exploit per una vulnerabilità già chiusa da Microsoft!	

II. Requisiti per i software di protezione utilizzati

Un sistema di protezione antivirus dovrebbe:

1. **avere la possibilità di rilevamento dei programmi malevoli precedentemente sconosciuti.** Gli autori di virus usano estensivamente il testing delle loro "opere" sui servizi specializzati, in seguito a cui la presenza in un antivirus dei soli meccanismi euristici non permette di garantire il rilevamento dei programmi malevoli più recenti. Il metodo più comune per nascondere firme antivirali già note è quello di rimpacchettare i programmi malevoli precedentemente creati, tra l'altro utilizzando formati dei packer con formati non conosciuti da un sistema di protezione. Per contrastare questo metodo, nelle soluzioni Dr.Web si utilizzano le tecnologie che hanno la possibilità di ricerca dei programmi malevoli conosciuti in forma rimpacchettata (**Dr.Web Fly-Code**), e inoltre gli strumenti di protezione proattivi che individuano i modelli di comportamento caratteristici dei programmi malevoli e non richiedono la conoscenza delle loro firme antivirali (**Protezione preventiva Dr.Web**).

2. **avere un sistema di auto-protezione affidabile** che non permette di essere disattivato dai programmi malevoli più recenti, né dai dipendenti che desiderano raggirare le regole di sicurezza aziendali. La presenza di tale sistema consente alle soluzioni antivirus di far fronte agli attacchi dei programmi malevoli ancora prima della ricezione degli aggiornamenti che bloccano la fonte di attacco.

3. **avere la possibilità di bloccare le disattivazioni della protezione antivirus.** Per questo scopo è necessario utilizzare la protezione centralizzata con la possibilità di limitare i permessi degli utenti a seconda delle loro responsabilità lavorative, e inoltre proteggere con password l'accesso alle impostazioni del sistema di protezione sulle postazioni che non hanno la gestione centralizzata.

4. **assicurare l'aggiornamento del software.** Il sistema di aggiornamento Dr.Web utilizza server situati in diverse parti del mondo. Le tecnologie di aggiornamento permettono di aggiornare tutte le postazioni del sistema protetto allo stesso tempo, senza alcun carico per la rete locale. L'utilizzo della protezione centralizzata permette di aggiornare le postazioni della rete secondo un calendario e di riavviare le postazioni in remoto, mentre la protezione con password dell'accesso alle impostazioni del sistema di protezione sulle postazioni che non hanno la gestione centralizzata esclude la possibilità di rifiutare gli aggiornamenti.

5. **assicurare l'aggiornamento della licenza.** Nei prodotti Dr.Web è incluso un sistema che permette di rinnovare le licenze automaticamente attraverso il fornitore del software antivirus.

III. Scelta delle misure di protezione

Un sistema di protezione antivirus dovrebbe non soltanto bloccare i programmi malevoli conosciuti, ma anche ostacolare la diffusione dei malware sconosciuti nella rete e oltre i suoi confini.

1. Dovrebbero essere protetti i nodi della rete locale su cui è possibile installare un antivirus — compresi i sistemi operativi del tipo Linux e Mac, i server di posta, i gateway Internet, i dispositivi mobili. Se i dipendenti utilizzano dispositivi personali e computer di casa, anch'essi dovrebbero essere protetti. Se si rinuncia alla protezione dei dispositivi mobili e dei computer personali, dovrebbero essere protetti i server di posta e i gateway Internet attraverso cui i dipendenti accedono ai servizi aziendali.
2. I sistemi in cui i programmi malevoli possono infiltrarsi (incluse le stampanti), ma in cui non è possibile installare sistemi antivirus, dovrebbero essere massimamente isolati dal resto della rete locale.

Un software di protezione antivirus delle postazioni utilizzato dovrebbe:

1) essere in grado curare i programmi malevoli non soltanto al momento della loro intrusione nel sistema, ma anche i programmi malevoli già avviati — precedentemente sconosciuti;
2) rilevare i campioni di programmi malevoli conosciuti, impacchettati in file con un formato sconosciuto;
3) avere la possibilità di impiegare meccanismi addizionali (oltre alle firme antivirali e all'analisi euristica) per il rilevamento dei programmi malevoli sconosciuti — tra le altre cose, un meccanismo di protezione preventiva e componenti cloud;
4) per proteggere dall'infiltrazione dei programmi malevoli non conosciuti al momento dell'infezione, comprendere:
   - un firewall personale che assicura l'impossibilità di scansione della rete locale e inoltre la protezione dagli attacchi all'interno della rete;
   - un sistema che limita l'accesso ai supporti rimovibili e alle risorse all'interno della rete, compresi i dischi rimovibili, alle directory e ai siti Internet;
   - un sistema centralizzato che esegue scansioni periodiche per accertare l'assenza dei programmi malevoli non attivi e delle vulnerabilità conosciute;
5) controllare tutti i file che arrivano dalla rete locale prima che vengano ricevuti dalle applicazioni in uso, il che esclude lo sfruttamento delle vulnerabilità sconosciute di queste applicazioni da parte dei programmi malevoli;
6) avere un sistema di auto-protezione che non permette a un programma malevolo sconosciuto di interrompere il normale funzionamento dell'antivirus — la soluzione antivirus dovrebbe funzionare normalmente fino a quando non arriverà un aggiornamento che consente di curare l'infezione;

7) avere un sistema di raccolta informazioni che permette di trasmette il più velocemente possibile all'laboratorio antivirus tutte le informazioni necessarie per risolvere un problema. Dovrebbero essere escluse le situazioni in cui in ciascun caso di infezione le informazioni richieste devono essere raccolte manualmente — in particolare, sulle postazioni remote e sui server;
8) posizionare i database antivirus utilizzati completamente nella RAM per evitare il caricamento (compreso il montaggio) da un disco rigido che provoca il rallentamento delle operazioni di verifica antivirus;
9) fornire una verifica multithread escludendo la formazione di una coda dei file in fase di scansione;
10) funzionare su sistemi operativi che non sono più supportati dal loro produttore;
11) per proteggere dai programmi malevoli sconosciuti che vengono trasmessi in messaggi di posta, utilizzare un antispam (antiphishing) che non richiede un continuo ulteriore addestramento;
12) escludere la necessità di configurazione manuale dei parametri di carico della CPU, utilizzando un sistema di analisi automatica del suo carico.

Un sistema di gestione centralizzata della protezione antivirus utilizzato dovrebbe:
1) similmente al sistema di aggiornamento della soluzione antivirus: essere indipendente dai relativi meccanismi utilizzati nei sistemi operativi; essere incluso nel sistema di auto-protezione dell'antivirus, il che permette di escludere la possibilità di intercettazione del sistema di aggiornamento da parte di un programma malevolo. Non è ammesso l'utilizzo da parte dell'antivirus di componenti di sistema non tutelati dal sistema di auto-protezione dell'antivirus;
2) utilizzare su tutte le postazioni e sui server un antivirus che comprende un analizzatore comportamentale proattivo e un firewall personale;
3) assicurare la ricezione più veloce possibile degli aggiornamenti da parte delle postazioni e dei server protetti — tra l'altro, con una decisione dell'amministratore, a scapito delle prestazioni complessive della rete locale protetta. La minimizzazione del tempo di ricezione di un aggiornamento dovrebbe, in particolare, essere assicurata dalla minimizzazione della dimensione degli aggiornamenti stessi, e inoltre da una continua comunicazione delle postazioni e dei server protetti con il server di aggiornamento;
4) avere la possibilità di applicare impostazioni individuali per gruppi e singoli utenti;
5) avere la possibilità di eseguire una verifica antivirus completa o personalizzata di un nodo della rete sia su comando dell'utente o dell'amministratore e sia secondo un calendario;
6) avere la possibilità di installare, aggiornare e configurare in maniera centralizzata i software di protezione antivirus, tra l'altro, sui nodi della rete non accessibili dal server;
7) essere in grado di funzionare nelle reti suddivise in singoli segmenti.

Oltre all'uso di un antivirus, è consigliato:
1. Introdurre una limitazione dei permessi degli utenti. Tra cui:
   1) rinunciare all'uso dei permessi amministratore sulle postazioni;
   2) limitare i permessi di accesso a risorse locali e di rete;
   3) limitare l'uso dei supporti rimovibili. In questo caso è necessario tenere presente che le white list dei dispositivi, di regola, non sono efficaci a causa del fatto che gli identificatori di tutti i dispositivi di una partita sono identici.

2. Utilizzare la suddivisione della rete locale in singoli segmenti isolati, installando un sistema di filtraggio del traffico trasmesso tra i segmenti.
3. Rimuovere prodotti, servizi e componenti non utilizzati.
4. Utilizzare un sistema di backup posizionato su un server separato.
5. Trasferire database su server separati con il divieto di accesso e utilizzare il controllo delle versioni di file e documenti conservati.
6. Impostare il divieto di accesso a Internet e alla rete locale per tutti i programmi tranne quelli consentiti.
7. Vietare l'utilizzo delle password di amministratore di dominio sulle postazioni.
8. Utilizzare l'installazione centralizzata di tutti gli aggiornamenti di sicurezza per tutti i prodotti in uso. Aggiornare con regolarità tutti i software installati sulle postazioni.

Per una verifica di emergenza delle postazioni potenzialmente infette dovrebbe essere utilizzato uno scanner antivirus di rete, e inoltre un disco / supporto rimovibile di avvio di antivirus.

IV. Dr.Web Enterprise Security Suite — complesso di prodotti per le imprese.

Per i clienti business l'azienda Doctor Web offre il suo prodotto di punta – il complesso Dr.Web Enterprise Security Suite il quale possiede molte caratteristiche uniche:

- protezione centralizzata di tutti i nodi di una rete – postazioni, server di posta e di file, server di applicazioni, tra cui terminal server, gateway Internet e dispositivi mobili.
- protezione completa delle postazioni dalla maggior parte delle minacce esistenti grazie alla presenza di un antivirus, un antispam, un monitoraggio http, un firewall e un office control;
- costo totale di dispiegamento minimo rispetto ai programmi concorrenti grazie alla possibilità di installare i server sia Windows che Unix, a un database incorporato, a un'installazione facile e a una protezione affidabile. Un'azienda non avrà bisogno di acquistare hardware costosi insieme a Dr.Web Enterprise Security Suite;
- possibilità di installare il software agent su una macchina già infettata ed elevata probabilità di guarigione;
- minimo impiego delle risorse dei computer e server grazie alle piccole dimensioni del motore antivirus e all'utilizzo in esso delle tecnologie più nuove;
- elevata efficacia di rilevamento delle minacce, compresi i virus non ancora conosciuti;
- gestione dell'intera infrastruttura di protezione della rete da una singola postazione di lavoro ovunque si trovi (attraverso l'Amministratore web);
- realizzazione dei criteri di sicurezza necessari per una particolare azienda o per singoli gruppi di dipendenti;
- assegnazione di amministratori separati a diversi gruppi, il che permette di utilizzare Dr.Web Enterprise Security Suite sia in aziende con elevati requisiti di sicurezza, che in imprese multisede;
- impostazione dei criteri di sicurezza per qualsiasi tipo di utente, inclusi gli utenti mobili, e per qualsiasi postazione – persino per una al momento assente dalla rete – consente di garantire in qualsiasi momento lo stato di sicurezza aggiornato;
- protezione di qualsiasi rete, compresa una rete senza l'accesso a Internet;
- possibilità di utilizzare la maggior parte dei database esistenti. Come i database esterni possono essere utilizzati Oracle, PostgreSQL, Microsoft SQL Server, qualsiasi DBMS con il supporto di SQL-92 tramite ODBC;
- possibilità di scrivere propri gestori eventi, il che dà accesso diretto alle interfacce interne del Pannello di controllo;
- chiarezza del sistema di controllo dello stato di protezione, efficienza e comodità ineguagliabili della ricerca delle postazioni;

- la possibilità di selezionare una lista dei componenti di un prodotto da aggiornare e quella di controllare il passaggio alle nuove versioni permettono agli amministratori di installare i soli aggiornamenti richiesti e provati nella loro rete.

Il complesso Dr.Web Enterprise Security Suite include i seguenti prodotti:

Dr.Web Desktop Security Suite – protezione di postazioni, di client di terminal server, di client di server virtuali e di client di sistemi embedded

Dr.Web Server Security Suite – protezione di file server e di server di applicazioni (compresi terminal server e server virtuali)

Dr.Web Mail Security Suite – protezione della posta

Dr.Web Gateway Security Suite – protezione di Internet gateway

Dr.Web Mobile Security Suite – protezione di dispositivi mobili

Dr.Web Enterprise Security Suite è presente nel Registro dei software russi e permette di rispettare tutti i requisiti della legislazione vigente nel campo della protezione antivirus.

Tutti i prodotti che fanno parte di Dr.Web Enterprise Security Suite possono essere utilizzati gratis per 30 giorni. Invitiamo le aziende a fare una richiesta di una licenza di prova e ad apprezzare l'affidabilità della protezione e la qualità del rilevamento e della cura infezioni Dr.Web.

Descrizione: https://products.drweb.com/enterprise_security_suite/?lng=en

Richiesta di una versione di prova: https://download.drweb.com/demoreq/biz/v2/?lng=en

L’azienda Doctor Web

Doctor Web – produttore russo dei software di protezione antivirus delle informazioni sotto il marchio Dr.Web. I prodotti Dr.Web vengono sviluppati fin dal 1992. L’azienda è un giocatore chiave sul mercato russo dei software studiati per soddisfare un’essenziale esigenza delle aziende – quella della sicurezza delle informazioni. Doctor Web è tra i pochi fornitori degli antivirus del mondo a possedere le proprie tecnologie uniche di rilevamento e cura dei programmi malevoli. La protezione antivirus Dr.Web consente ai sistemi informatici dei clienti di resistere efficacemente ad ogni minaccia, persino ad una non ancora conosciuta.
Doctor Web è stata la prima azienda ad offrire sul mercato russo il modello innovativo di antivirus come un servizio e fino ad oggi continua ad essere il leader indiscusso del mercato russo dei web service di sicurezza progettati per i fornitori dei servizi IT. I certificati e i premi statali e la geografia degli utenti di Dr.Web confermano l’alta qualità dei prodotti creati dai programmatori russi di talento.

125040, Russia, Mosca, la 3° via Yamskogo polya, 2, 12a

Telefono: +7 (495) 789–45–87 (centralino)

Fax: +7 (495) 789–45–97