Dr.WEB®
dal 1992

Falsi miti sugli antivirus

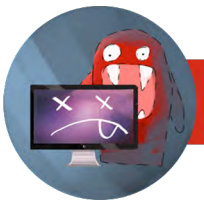
Falsi miti sugli antivirus

Quasi ogni utente moderno del computer o del dispositivo mobile qualche volta si è trovato di fronte alle conseguenze delle azioni dei programmi malevoli o almeno ha letto o sentito di tali conseguenze. Eppure "tutti lo sanno" che "i virus vengono scritti dagli sviluppatori degli antivirus", che "non esistono programmi malevoli per Linux e Mac", e che "sotto Android soltanto l'utente stesso potrebbe installare un virus per l'inesperienza". È vero?

Se si crede ai falsi miti, se si è riluttanti a percepire le informazioni oggettive e a fare da esse corrette conclusioni, se si rifiuta di riconoscere i fatti e si cade nell'autoinganno nei loro riguardi – tutto questo porta a pericolose idee sbagliate.

Le idee sbagliate potrebbero portare a decisioni sbagliate e talvolta a gravi conseguenze.

Questa brochure è dedicata ai falsi miti che circondano gli antivirus, alle ragioni per cui sono sorti e alla loro influenza sulla sicurezza informatica di ogni utente di antivirus.



Falso mito No. 1. I virus non esistono

Non è vero, qui è importante distinguere tra i virus veri e propri, capaci di replicarsi da soli, e gli altri programmi malevoli. I visus esistono, ma ce ne sono assai pochi rispetto ai trojan adesso diffusi.

Nella definizione rigorosa del termine, i virus sono programmi malevoli auto-replicanti — cioè sono in grado di creare le loro copie e di introdurre il loro codice in altri file.

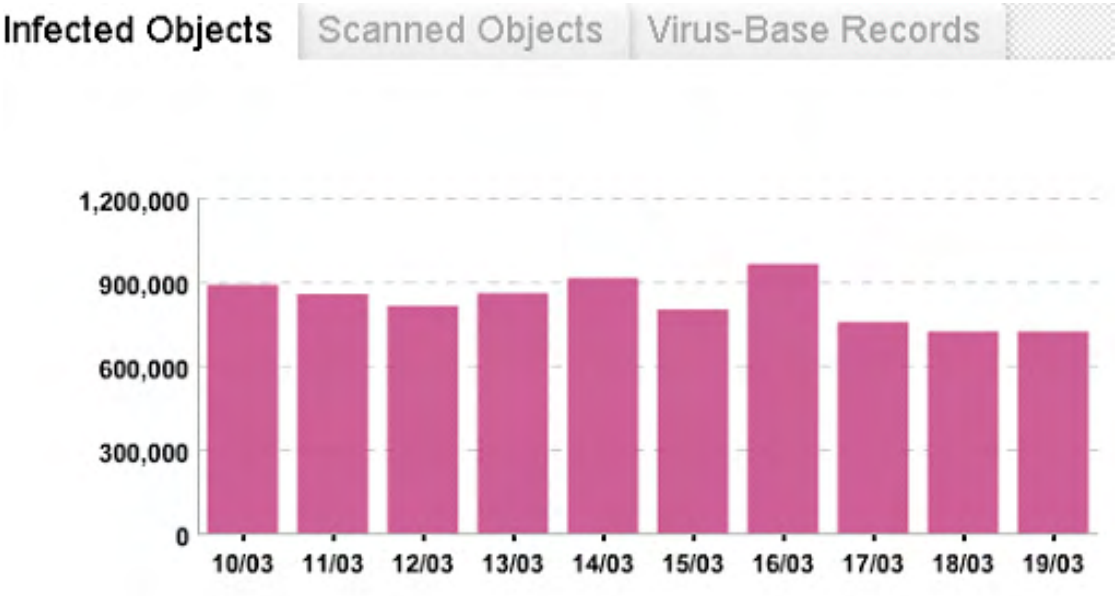
Oggi la stragrande maggioranza di programmi malevoli (oltre il 90%) è trojan. I trojan non hanno il meccanismo di auto-replicazione e non sono virus.

Falso mito No. 2. Nuovi programmi malevoli compaiono di rado

Persino alcuni specialisti informatici pensano che la quantità di programmi malevoli creati al giorno sia attorno ad un centinaio. In realtà, ciò è ben lungi da essere vero.

Nei laboratori dei virus arrivano fino ai **venticinque milioni di campioni potenzialmente dannosi al mese.**

Numero di campioni arrivati nel Laboratorio dei virus Doctor Web a marzo 2015.

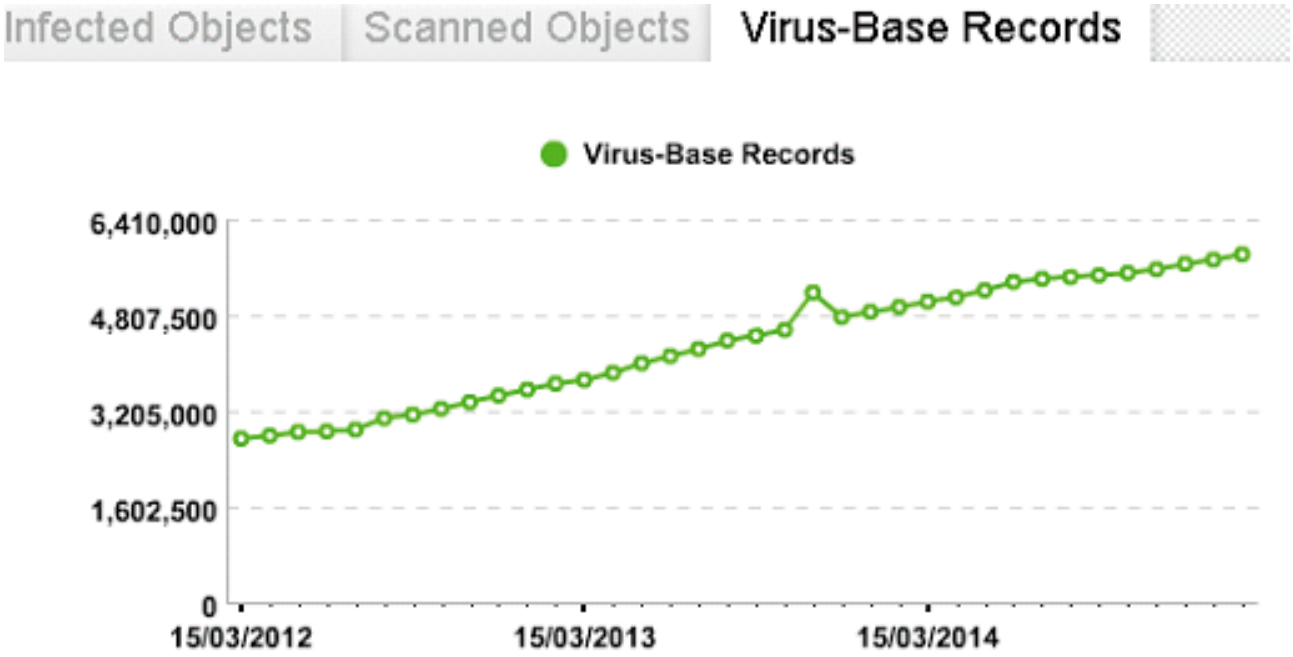


Non tutti i campioni sono programmi malevoli. E, naturalmente, alcuni campioni si ripetono. Però tutti devono essere elaborati dai nostri specialisti.

Elaborare manualmente diversi milioni di campioni al mese è un compito impossibile.

La maggior parte dei campioni viene elaborata dai bot specializzati. Gli analisti dei virus esaminano soltanto i campioni complessi di cui l'elaborazione automatica non è possibile. Il database dei virus Dr.Web si accresce ogni ora.

Aumento del numero di record nel database dei virus Dr.Web



Falso mito No. 3. Le aziende antivirus stesse scrivono programmi malevoli

Molti utenti pensano che i virus vengano scritti dagli sviluppatori degli antivirus stessi visto che possono trarre vantaggio dalla loro esistenza — se non ci saranno dei virus, gli utenti non compreranno gli antivirus.

Questo è il nostro mito preferito! Ed è anche il più tenace tra tutti i falsi miti sugli antivirus. Non passa un mese senza che qualcuno non ci abbia scritto di questa convinzione tramite il nostro modulo di feedback.

Il mito deriva logicamente dalle supposizioni che:

1. il numero di programmi malevoli creati al giorno sia assai piccolo,
2. possano essere scritti da alcuni specialisti e
3. questi specialisti lavorino, naturalmente, nelle aziende antivirus.

- Il numero di programmi malevoli sviluppati dai malfattori è così grande che i laboratori dei virus sono sovraccaricati di lavoro a tre turni 7 giorni alla settimana. Scrivere programmi malevoli in tale situazione non ha senso, ci si augura di riuscire a far fronte a quelli che vengono per l'analisi da fuori.
- Per uno specialista della sicurezza informatica, creare un programma malevolo è una cosa assolutamente inutile, prima di tutto perché se il record di rilevamento di questo programma trojan verrà aggiunto ai database dell'antivirus che lui stesso sviluppa, gli utenti già saranno protetti da questa minaccia fin dall'inizio, e tra un breve tempo il trojan verrà incluso anche nei database degli altri programmi antivirus. Perché perdere tempo inutilmente?
- La creazione di software malevolo è un reato penale. Se diventasse noto che qualcuno sviluppa virus, la persona rischierebbe di finire dietro le sbarre. E la cosa sicuramente diventerà nota – gli analisti dei virus hanno parecchi detrattori.
- I vendor antivirus non soltanto che non scrivono virus, ma persino non spediscono file malevoli già conosciuti per scopi di test, una cosa che ci chiedono di volta in volta clienti che vogliono testare nuovo software o giornalisti che vogliono fare un confronto. Se mai diventasse noto che un'azienda o un suo dipendente si sono occupati di creazione o semplicemente di diffusione di software malevolo, il business di quest'azienda verrebbe cancellato.
- Molti produttori dei programmi per la protezione antivirus — e tra questi l'azienda Doctor Web — non assumono coloro i quali in un modo o nell'altro si occupavano di pirateria e intrusione informatica. Una persona che mai è stata coinvolta nella creazione di virus ha un basso livello di moralità.

Chi in effetti scrive i programmi malevoli?

All'alba dell'era del computer, i programmi malevoli effettivamente venivano creati soprattutto per esprimere la creatività e la personalità del programmatore. Anche adesso capita che i programmi malevoli vengano scritti da singole persone che sognano la fama, ma non essi rappresentano il principale pericolo.

Non è soltanto che i programmi malevoli moderni vengono sviluppati da autori di virus professionali. Ma è che adesso tale programmazione è parte di un business criminale ben organizzato.

Le comunità criminali includono:

- Organizzatori — persone che avviano il processo della creazione e dell'utilizzo del software malevolo e gestiscono questo processo.
- Sviluppatori del software malevolo.
- Tester del software malevolo.
- Ricercatori – cercano vulnerabilità nei sistemi operativi e programmi applicativi, adatte per uso criminale.
- Distributori del software malevolo.
- Amministratori che provvedono al lavoro distribuito sicuro all'interno della comunità criminale e gestiscono botnet.
- Webmaster che creano siti per la distribuzione del software malevolo.
- Venditori che realizzano programmi malevoli (alcuni trojan vengono scritti per la vendita o l'affitto).
- Organizzatori degli attacchi DDoS.
- Creatori delle risorse pubblicitarie e dei partner program non affidabili che permettono di guadagnare, utilizzando i trojan che visualizzano pubblicità.

Grazie alla buona organizzazione delle comunità criminali, che sviluppano e distribuiscono malware, la produzione dei programmi malevoli avviene a flusso. Questa circostanza ha provocato una crescita esplosiva del numero di programmi malevoli creati dai malfattori e quindi ha influito sul numero di firme antivirali aggiunte ai database dei virus ogni giorno.

Il numero di programmi, rilasciati da una comunità criminale, può raggiungere diverse centinaia di campioni al giorno — e nessuno di essi, per un tempo dopo il rilascio, verrà rilevato dal software antivirus utilizzato dal gruppo target delle vittime. Perché – lo spiegheremo più avanti.

Con quale scopo vengono scritti i programmi malevoli?

Il software malevolo viene creato esclusivamente con lo scopo di profitto.

È un criminale chi è coinvolto nel processo di creazione, distribuzione e supporto dell'infrastruttura per il funzionamento di un trojan creato per rubare qualcosa.

I trojan moderni rubano sia informazioni e sia beni materiali degli utenti e delle aziende. Qualsiasi cosa rubata potrà successivamente essere rivenduta:

- Login e password — credenziali di accesso ai sistemi di online banking e di pagamenti elettronici, ad account in social network e così via.
- Denaro virtuale (per esempio bitcoin).
- Messaggi di email e indirizzi dalla rubrica.
- Fotografie — si possono usare per ricattare la potenziale vittima o per causarle il danno morale pubblicando le foto in Internet.
- Qualsiasi sorta di informazione tecnica su PC della vittima.
- Account e oggetti virtuali di gioco.

Se non c'è niente da rubare su un computer, può essere utilizzato per la creazione di una botnet.

Attenzione!

In alcuni paesi il proprietario del computer coinvolto in una botnet e utilizzato per attaccare altri computer o siti web può essere chiamato a responsabilità penale — anche se non ne sapeva nulla.

Falso mito No. 4. L'antivirus deve rilevare tutti i programmi malevoli al momento quando si infiltrano nel computer

È molto tenace questo falso mito. Ma la cosa è semplicemente impossibile! Così com'è impossibile inventare un farmaco che possa curare tutte le malattie alla volta. La panacea per tutti i mali non esiste e ci si deve rassegnare sebbene per secoli sia stata un sogno dell'umanità.

Il mito persiste perché la maggior parte degli utenti non sa com'è organizzata l'impresa criminale dei produttori dei virus. Uno dei principali processi nella creazione di un trojan "buono" (cioè invisibile all'utente e al suo antivirus) è il **collaudo del programma malevolo contro il rilevamento** dalla maggior parte degli antivirus popolari.

> *Viene rilasciato o introdotto sul PC della vittima (se l'attacco ha un bersaglio preciso) soltanto quel trojan che non viene rilevato da nessun programma di sicurezza.*

Pertanto, intercorre un intervallo tra il rilascio di un trojan dai malintenzionati e il momento quando un suo campione viene analizzato nel laboratorio dei virus e viene rilasciato un "antidoto". Anche se questo vale solo per i trojan veramente complessi e "di successo". La maggior parte dei programmi malevoli comuni viene rilevata tramite le firme antivirali, nonché tramite l'analisi euristica e le altre tecnologie non basate su firme antivirali del nucleo antivirus Dr.Web.

Falso mito No. 5. L'attività di un virus sul computer è sempre visibile.

Questo mito è uno dei più pericolosi! È radicato nei tempi dei primi virus, la maggior parte dei quali aveva le funzioni distruttive, ad esempio cancellava tutte le informazioni sul PC oppure si manifestava con tanta operosità — ad esempio il virus inviava in massa email con la sua copia, il che rallentava notevolmente il sistema così che l'utente poteva accorgersene.

> *Oggi gli intrusi sono interessati ai vostri soldi e dati. Per rubarli, il virus deve rimanere quanto più possibile nascosto.*

A proposito:

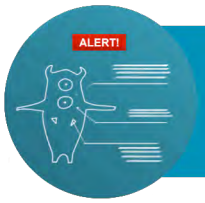
1. Dopo che è avvenuta l'infezione, alcuni programmi malevoli eliminano le falle nel sistema attraverso cui potrebbero penetrare altri programmi malevoli e ripuliscono il sistema da quelli già presenti.

2. Alcuni trojan "uccidono" l'antivirus (cioè terminano i suoi processi nel sistema) e quindi mettono la sua icona nell'area di notifica della barra delle applicazioni di Windows per dare all'utente l'impressione che l'antivirus sia ancora in esecuzione per far abbassare la sua vigilanza. Le risorse di tale programma malevolo includono le icone di tutti gli antivirus popolari, e il trojan intelligente ne seleziona quella che corrisponde all'antivirus installato sul PC sotto attacco. Tale icona non risponde naturalmente ai clic del mouse e ad altri tentativi di influenza e l'antivirus sembra di essere bloccato. In realtà, la macchina è senza protezione. Dr.Web ha un apposito sistema di auto-protezione contro tali attacchi.

Quindi non illudetevi — gli autori dei virus hanno capito da lungo tempo che il migliore trojan è un trojan invisibile all'utente.

Il mito però rimane vivo come nessun altro.

E questa credenza porta a conseguenze veramente tristi. Le persone che credono a questo mito non utilizzano alcun antivirus o non ritengono che sia necessario attenersi alla regola di base dell'utilizzo dell'antivirus, cioè eseguire scansioni a cadenze regolari.



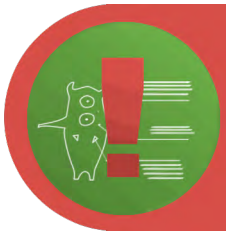
Falso mito No. 6. L'antivirus individua programmi malevoli solo sulla base delle firme antivirali

Il mito vive dai primi anni dell'esistenza degli antivirus. Allora, più di 20 anni fa, questo fu davvero così.

Gli antivirus che individuano programmi malevoli solo sulla base delle firme antivirali si estinsero negli anni 90 del secolo scorso quando furono comparsi i virus polimorfici che mutano ad ogni avvio e quindi non possono essere rilevati tramite le firme antivirali (a proposito, proprio questo portò alla comparsa dell'antivirus russo Dr.Web).

Se anche oggi un antivirus fosse in grado di riconoscere nuovi virus soltanto tramite i record nei database dei virus, tali database non sarebbero entrati tutti nella memoria di nessun computer, la scansione avrebbe impiegato tanto tempo e le prestazioni del PC sarebbero gravemente diminuite.

> *Un antivirus moderno è un complesso di tecnologie euristiche, comportamentali e preventive, non basate su firme antivirali, che tutte,* **insieme ai record dei database dei virus**, *consentono all'antivirus di proteggere l'utente dalle minacce reali.*



Falso mito No. 7. Se non c'è un record per un programma malevolo nel database dei virus, l'antivirus deve riconoscerlo tramite le tecnologie euristiche

Il mito esiste perché ne esiste un altro, quello che un antivirus debba individuare il 100% dei programmi malevoli, e viene sostenuto dai test che valutano il rilevamento tramite l'analisi euristica.

> *In effetti, l'analisi euristica rileva* **solo le nuove varianti dei programmi malevoli già esaminati di cui il comportamento è conosciuto dall'antivirus.**

Se un trojan viene incluso nei database dei virus, i suoi autori, per evitare la necessità di modificarlo, lo ricomprimono tramite un programma packer o lo cifrano.

Cosa in tal caso deve fare l'antivirus? La prima possibilità è aggiungere ogni nuovo campione nel database dei virus (probabilmente, alcuni antivirus fanno proprio questo!), mentre la seconda possibilità è catturare virus tramite la tecnologia FLY-CODE e l'analisi dell'entropia di struttura, come lo fa Dr.Web. La tecnologia FLY-CODE controlla oggetti eseguibili compressi, decomprime file pacchettati da packer non-standard tramite la virtualizzazione dell'esecuzione del file, mentre l'analisi dell'entropia di struttura rileva minacce sconosciute sulla base della posizione dei tratti di codice negli oggetti compressi e criptati.

Il compito dell'antivirus è sia prevenire l'infezione e sia curare il pc dai programmi malevoli già penetrati.

Purtroppo, l'antivirus non può rilevare tutti i programmi malevoli al momento quando avviene l'infezione. Perciò per prevenire l'infezione, altri sistemi vengono in soccorso dell'antivirus — tra cui i sistemi di limitazione di esecuzione dei programmi sconosciuti e di controllo del comportamento.

Soltanto l'antivirus però può curare il sistema dai programmi malevoli penetrati ed attivi che ostacolano i tentativi dell'eliminazione da parte dei sistemi di protezione.

Nessun prodotto software, salvo l'antivirus, è in grado di guarire il sistema infettato da un programma malevolo. La cura è una missione possibile soltanto per l'antivirus e no per alcun altro prodotto software.

Falso mito No. 8. Per proteggersi contro i programmi malevoli, occorrono altri software oltre all'antivirus

L'antivirus moderno è in grado di rilevare sia il software spia che i rootkit e non richiede alcun software addizionale per aiutarlo. Inoltre, il set di consegna di alcuni antivirus include un firewall – apposito componente capace di proteggere il computer da accessi non autorizzati in rete.

L'antivirus trova ed elimina dal sistema ogni genere di software malevolo. All'antivirus non serve l'aiuto di alcun altro prodotto software.

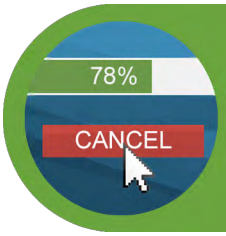
Oltre ai veri antivirus, esistono programmi che si spacciano per antivirus o per altro software di sicurezza. In molti casi non è che sono semplicemente inutili, ma è che infettano i PC degli utenti che si sono fidati della pubblicità.

Non importa quanto sia cauto un utente, corre comunque il rischio di prendersi un virus sul computer attraverso le vulnerabilità in prodotti software o potrebbe rimanere vittima del social engineering e dei trucchi dei phisher.

Per esempio, proprio alcune vulnerabilità facilitarono la vasta diffusione della prima epidemia sui computer Mac OS X, quella del trojan **BackDoor.Flashback.39**. Per diffondere il trojan, i malfattori utilizzarono diverse vulnerabilità nella macchina virtuale Java, **come conseguenza:**

650.000 computer Mac

vennero infettati dal BackDoor.Flashback in tutto il mondo.



Falso mito No. 9. Se l'utente non visita siti non attendibili e non apre link in email arrivate da mittenti sconosciti, l'antivirus non è necessario

Gli utenti che credono che l'antivirus non sia necessario e soltanto rallenti il computer, pensano che il sistema possa essere infettato solo se l'utente installa un trojan con le proprie mani — per esempio, scaricandolo attraverso un link malevolo da un'email.

Tuttavia, la pratica mostra: in un enorme numero di casi gli utenti stessi scaricano e installano un trojan sui loro PC senza nemmeno accorgersene!

Inoltre, esistono scenari di attacco quando non è necessario che l'utente faccia alcunché per lanciare un trojan. In un istante un trojan invisibile può installarsi sul PC senza la partecipazione dell'utente che ne rimane all'oscuro.

Falso mito No. 10. L'antivirus non è necessario se il computer si usa solamente per giochi

L'industria moderna dei giochi per computer è un mercato altamente sviluppato con un giro d'affari annuo di decine di miliardi di dollari. E i giocatori non sono immuni alle minacce provenienti da Internet

Quando gli utenti potenziano i loro personaggi, talvolta acquistano artefatti per soldi reali – a questo punto possono aspettarsi delle brutte sorprese nella forma di un trojan. Per esempio il **Trojan.SteamBurglar.1** *che è capace di rubare oggetti di gioco di un utente per la successiva vendita.*

Oltre ai trojan, esistono tanti metodi fraudolenti per costringere un giocatore a cedere i preziosi artefatti e persino il suo account, per includere il suo PC in una botnet e coinvolgerlo in un attacco DDoS al server di gioco di un'azienda concorrente ecc.

Il quadro è completato dai trojan-encoder che cercano sul PC vittima tracce di giochi online o di un account in Steam e cifrano file, chiedendo il pagamento di un riscatto.

L'antivirus proteggerà dall'infezione da tali programmi e il monitor http SpIDer Gate non consentirà di entrare su un sito fraudolento.

Affidate la protezione delle vostre risorse d'informazione al software Dr.Web

Certificati del Ministero della Difesa della Federazione Russa, licenze del Servizio di Sicurezza Federale e del Servizio di Controllo Tecnico e d'Esportazione della Russia per l'esecuzione di lavori concernenti il segreto di stato.

Tutti i diritti sulle tecnologie Dr.Web appartengono alla società russa «Doctor Web». I diritti d'autore sulle tecnologie Dr.Web appartengono a Igor Danilov — l'autore dell'antivirus Dr.Web e l'unico proprietario della società «Doctor Web».

Siamo tra i pochi vendor antivirus del mondo che possiedono le proprie tecnologie uniche di rilevamento e di neutralizzazione di programmi malevoli, abbiamo il proprio laboratorio antivirus, il servizio di monitoraggio di virus globale e il servizio di supporto tecnico.

Qualità superiore

Dr.Web è stato certificato dal Ministero della Difesa della Federazione Russa. La società «Doctor Web» ha le licenze del Servizio di Sicurezza Federale e del Servizio di Controllo Tecnico e d'Esportazione della Russia per l'esecuzione di lavori concernenti il segreto di stato. I certificati e i premi statali e la geografia degli utenti di Dr.Web comprovano l'alta qualità dei prodotti creati dai programmatori russi di talento.

Tutte le licenze e i certificati di Doctor Web

Doctor Web, 2003 – 2015

Russia, 125124, Mosca, via 3 Yamskogo Polya, tenuta 2, edificio 12A
Telefono: +7 (495) 789-45-87 (centralino)
Fax: +7 (495) 789-45-97

www.drweb.com | www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com