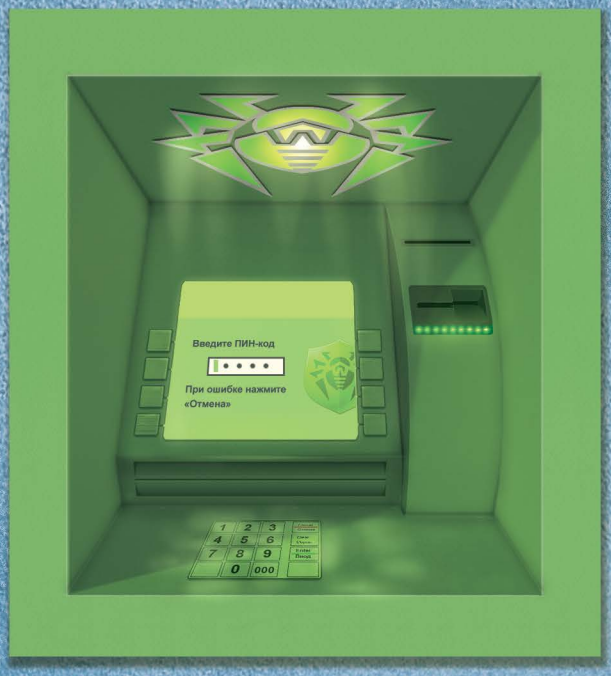
Dr.WEB®
ATM Shield



Protezione centralizzata
dei sistemi embedded
(sportelli automatici, terminali e reti POS ecc.)

A marzo 2009 in Russia fu scoperto il primo programma malevolo che infetta i bancomat. I bancomat infettati dal Trojan.Skimer furono rilevati prima a Mosca e quindi a San Pietroburgo.

In questa situazione l'azienda Doctor Web reag per prima, diede la notizia del Trojan.Skimer e in seguito cre un apposito antivirus dedicato alla protezione in tempo reale dei sistemi embedded (bancomat, terminali e reti POS ecc.), ovvero **Dr.Web ATM Shield.**

Dr.WEB®
ATM Shield

Ammettete che anche voi:

- Utilizzate i dispositivi USB senza eseguire prima una scansione antivirus?
- Aprite le email arrivate da mittenti sconosciuti?
- Utilizzate Windows con i permessi dell'amministratore?
- Non scaricate gli aggiornamenti di sicurezza di tutti i programmi installati sul pc?
- Vi connettete a Internet dal computer d'ufficio su cui sono installati alcuni programmi che hanno vulnerabilit ?
- Utilizzate password semplici e facili da scoprire?

Ma perché pensate che il personale addetto alla manutenzione dei bancomat si comporta in modo diverso?

I virus per i bancomat esistono?

I virus – programmi capaci di riprodursi da soli – ideati per l'infezione dei bancomat non sono ancora conosciuti. Però esistono molti programmi-trojan per bancomat e il loro numero sta aumentando di continuo! In un solo mese – dicembre 2013 – sono emersi quattro trojan per bancomat nuovi: Trojan.Ploutus.1, Trojan.Ploutus.2, Trojan.Skimer.19 e Trojan.PWS.OSMP.21.

Alcune caratteristiche dei trojan per bancomat:

- il programma malevolo viene gestito con l'ausilio di una master card sul bancomat e mediante un cellulare;
- intercetta e decifra il codice PIN inserito dal titolare di una carta bancomat **sfruttando il software del bancomat**;
- ruba le informazioni memorizzate sulla carta bancaria dell'utente; salva le informazioni rubate su un'apposita carta utilizzata dai malintenzionati oppure le stampa nello scontrino;
- consente di prelevare i contanti dal bancomat sulla base di un comando impartito dai malintenzionati dal PIN pad del bancomat o tramite un sms formato in un apposito modo.

Della manutenzione degli ATM si occupano i professionisti, dunque come un malware riesce a entrare?

Un bancomat può essere infettato tramite:

- **dispositivi rimovibili** utilizzati per la manutenzione ordinaria dei bancomat dal personale addetto, il quale però potrebbe utilizzare questi dispostivi anche per scopi privati;
- **dispositivi rimovibili** dei malintenzionati: per poterli utilizzare i criminali aprono l'apparecchio con un'apposita chiave;
- alcuni malware potrebbero penetrare nel bancomat dalla **rete interna aziendale** già infettata, in caso di disponibilità della connessione con i sistemi embedded;
- **vulnerabilità** presenti nel software del bancomat.

Anche se il malware penetrato nel bancomat sarà un programma comune non progettato per le manipolazioni con il denaro e le carte bancarie, potrebbe procurare problemi, per esempio la schermata blu o la cifratura delle informazioni seguita dalle richieste di pagare per la possibilità di riaverle. Probabili conseguenze: fotografie del bancomat guastato messe in Internet e perdita di reputazione — questa non è soltanto una situazione sgradevole, implica spese per il ripristino della normale operatività dell'apparecchiatura.

Dr.Web ATM Shield – non è soltanto un antivirus!

Dr.Web ATM Shield include i componenti che limitano notevolmente la probabilità di infezione (accidentale o intenzionale) del bancomat:

- un file monitor che impedisce l'avvio dei programmi malevoli conosciuti;
- un modulo antirootkit che permette di rilevare le minacce prima sconosciute;
- un modulo Office control che limita la possibilità di utilizzo delle cartelle locali e dei siti di Internet, il che non consentirà all'eventuale malware di trasmettere dati al suo "proprietario" o di connettersi al server di controllo;
- proibisce l'utilizzo dei dispositivi rimovibili per escludere la possibilità di introduzione di un programma malevolo da un dispositivo rimovibile estraneo;
- un sistema di controllo del traffico dati che permette la connessione a Internet soltanto ai programmi consentiti e sulle porte consentite.

Dr.WEB®
ATM Shield

Dr.Web ATM Shield è progettato per la difesa contro le tipiche minacce per dispositivi embedded

Perché utilizzare una soluzione dedicata se si può installare un solito antivirus?

Le caratteristiche dei dispositivi embedded sono:

- piccola quantità di memoria operativa e un processore relativamente debole;
- necessità di un funzionamento continuo senza riavvio;
- utilizzo dei sistemi operati per i dispostivi embedded oltre ai soliti sistemi operativi.

Dr.Web ATM Shield è progettato per l'operazione sulle configurazioni hardware poco potenti

512 MB di memoria operativa sul dispositivo embedded è sufficiente per l'operatività di **Dr.Web ATM Shield**.

I prodotti Dr.Web, compreso **Dr.Web ATM Shield**, si distinguono per i database dei virus compatti e per la piccola dimensione degli aggiornamenti, quindi sono adatti per la protezione dei dispositivi remoti che hanno la connessione a Internet e alla rete aziendale a banda stretta.

Dr.Web ATM Shield supporta i sistemi operativi per i dispositivi embedded

Dr.Web ATM Shield può essere utilizzato non soltanto sotto i sistemi operativi normali come Windows® XP Professional, Windows® Vista, Windows® 7 e Windows® 8, ma anche sotto Windows® XP Embedded, Windows® 7 Embedded, Windows® 8 Embedded.

Dr.Web ATM Shield non è soltanto un antivirus! Include anche:

- tecnologie che consentono di minimizzare il tempo di controllo e di caricamento (grazie alla scansione multi-thread e al controllo differito dei file aperti per lettura;
- funzionamento stabile del sistema anche sui computer con una configurazione datata;
- kernel antivirus moderno che consente di rilevare e neutralizzare i virus nuovi non ancora registrati nel database dei virus, compresi quelli impacchettati tramite programmi-packer sconosciuti;
- auto-protezione elevata che non dà ai virus la possibilità di mettere il sistema fuori servizio.

Dr.Web ATM Shield è l'unica soluzione che tiene conto delle caratteristiche dei sistemi embedded

Attenzione!

Il furto di denaro con l'ausilio di programmi malevoli è un reato.

La società Doctor Web offre servizi di perizia degli incidenti informatici provocati dai virus, nonché di valutazione psicologica del personale al fine di rivelare favoreggiamento reale / personale / incoraggiamento di atti illegali, omissioni o negligenza.

http://antifraud.drweb.com/expertise/

Sul sito di Doctor Web, nella sezione delle informazioni giuridiche http://legal.drweb.com/?lng=en/ sono reperibili esempi di denunce da sporgere alla polizia o ad altre autorità e consigli su come comportarsi se si è scoperto un furto. Vi invitiamo a utilizzare queste informazioni!

Società Doctor Web

Doctor Web è un'azienda russa per la sicurezza informatica, produttrice degli antivirus Dr.Web.

I prodotti Dr.Web vengono sviluppati fin dal 1992. Doctor Web, una tra le maggiori aziende di software di sicurezza sul mercato russo, produce programmi che sono capaci di soddisfare un'esigenza essenziale dell'impresa odierna — quella della sicurezza dell'informazione. Doctor Web è tra i pochi produttori di software antivirus nel mondo che hanno tecnologie uniche proprie di rilevamento e di neutralizzazione di programmi malevoli. La protezione antivirus Dr.Web consente ai sistemi informativi dei nostri clienti di contrastare efficacemente tutte le minacce informatiche, persino quelle sconosciute.

Doctor Web è stata la prima azienda che ha lanciato sul mercato russo il modello innovativo di distribuzione dell'antivirus come servizio e oggi è il leader incondizionato del mercato dei web service di sicurezza forniti ai provider dei servizi IT. I programmi Dr.Web, creati da esperti programmatori russi, hanno acquistato la fiducia degli utenti in diversi paesi del mondo e hanno ricevuto molteplici premi e certificati di approvazione dello stato grazie alla loro elevata qualità.

Tra i clienti della società Doctor Web vi sono grandi aziende conosciute in tutto il mondo, banche russe ed internazionali, enti statali, scuole, università e istituzioni di ricerca scientifica, le cui reti locali includono decine di migliaia di computer. I programmi Dr.Web vengono utilizzati dalle autorità statali russe e dalle aziende del settore energia e combustibile.

125124, Mosca, la 3° via Yamskogo polya, 2-12A
Tel: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
http://www.drweb.com | http://www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com