



# Dr.WEB®

## ATM Shield



### La protection centralisée des systèmes embarqués

(DAB, GAB, terminaux de paiement, multi  
kiosques, caisses)

Le premier logiciel malveillant infectant les DAB a été découvert en Russie en Mars 2009. Les DAB infectés par le Trojan.Skimmer ont d'abord été découverts à Moscou, puis à Saint-Petersbourg.

Doctor Web a été le premier à réagir. L'éditeur a **informé les utilisateurs sur le Trojan.Skimmer**, puis a développé un antivirus spécial pour la protection des systèmes intégrés (DAB, GAB, terminaux de paiement, multikiosques) – **Dr.Web ATM Shield.**

### Il arrive que l'on fasse des choses sans en réaliser les risques :

- Utiliser des clés USB sans les analyser.
- Ouvrir les emails envoyés par des expéditeurs inconnus.
- Utiliser des ordinateurs sous Windows avec les privilèges administrateur.
- Ne pas effectuer les mises à jour des logiciels installés sur l'ordinateur.
- Accéder à Internet en utilisant l'ordinateur sur lequel sont installés des logiciels, qui, malheureusement, comportent des vulnérabilités.
- Utiliser des mots de passe faibles, qui sont faciles à pirater.

## Pensez-vous que le personnel qui effectue la maintenance des DAB et des terminaux de paiement ne fait pas les mêmes choses ?

### Y a-t-il des virus ciblant les DAB ?

Les spécialistes n'ont pas encore découvert de virus ciblant les DAB (des logiciels malveillants capables de se répliquer). Mais le nombre de Trojan ne cesse de croître ! Par exemple, pour le seul mois de décembre 2013, 4 nouveaux Trojans ciblant les DAB ont été découverts : Trojan.Ploutus.1, Trojan.Ploutus.2, Trojan.Skimer.19 et Trojan.PWS.OSMP.21.

#### Certaines particularités des Trojans ATM :

- le logiciel malveillant est géré à l'aide de cartes master spécialement conçues ou à l'aide d'un appareil mobile ;
- Les codes PIN sont interceptés et décryptés à l'aide des logiciels du DAB ! ;
- le vol des données des cartes bancaires ; la sauvegarde de ces données sur une carte spéciale ou l'impression des données sur un ticket ;
- Le retrait de billets sur commande des malfaiteurs, envoyée via le clavier du DAB ou un SMS spécial.

### Comment est-il possible d'infecter les DAB dont la maintenance est assurée par des professionnels ?

#### Les infections sont possibles :

- via les supports amovibles, utilisés lors des travaux de maintenance ;
- via les supports amovibles des malfaiteurs qui peuvent accéder au système du DAB à l'aide d'une clé spéciale ;
- depuis le réseau interne dans le cas où les systèmes intégrés sont accessibles depuis le réseau ;
- via les vulnérabilités dans les logiciels du DAB.

Même si le DAB est infecté par un logiciel malveillant " standard " qui n'est pas spécialement conçu pour pirater les cartes bancaires, les dommages qu'il peut entraîner comme un écran bleu sur le DAB ou le cryptage de données avec demande de rançon peuvent nuire à la réputation de la banque et entraîner des dépenses pour la restauration de l'équipement.

## Dr.Web ATM Shield — n'est pas seulement un antivirus !

#### Dr.Web ATM Shield comprend des fonctionnalités qui peuvent limiter les possibilités d'infecter les DAB :

- Le moniteur de fichiers rend impossible le lancement de menaces connues ;
- L'Anti-rootkit détecte les menaces inconnues ;
- Le module Office Control limite l'accès aux répertoires locaux et ressources Internet, ce qui empêche le malware de se connecter au serveur de gestion afin de transmettre les données volées ;
- l'interdiction de l'utilisation des supports amovibles protège contre la pénétration via les supports inconnus
- le contrôle du trafic web autorise la connexion Internet pour un nombre limité de logiciels.

**Dr.Web ATM Shield est développé pour résister aux menaces ciblant les systèmes embarqués.**

**Pourquoi faut-il utiliser une solution spéciale, s'il est possible d'installer un antivirus standard ?**

**Les caractéristiques des appareils embarqués sont les suivantes :**

- peu de RAM et un CPU faible ;
- fonctionnement 24 sur 24 sans les redémarrages ;
- des OS standards ainsi que des versions embedded.

**Dr.Web ATM Shield est spécifiquement conçu pour fonctionner sur les systèmes peu puissants.**

Dr.Web ATM Shield requiert 512 Mo de RAM.

Dr.Web ATM Shield, comme les autres produits Dr.Web, fournit des mises à jour des composants et bases virales de petite taille, ce qui permet de protéger les appareils ayant une faible connexion Internet.

**Dr.Web ATM Shield est compatible avec les versions embedded des systèmes d'exploitation.**

Dr.Web ATM Shield est compatible avec les OS suivants : Windows® XP Professional, Windows® Vista, Windows® 7 et Windows® 8, ainsi que Windows® XP Embedded, Windows® 7 Embedded, Windows® 8 Embedded.

## Dr.Web Shield ATM — n'est pas seulement un antivirus !

**Ce sont :**

- des technologies pour réduire les délais d'analyse et de démarrage (y compris grâce à la technologie d'analyse multi flux et le report de scan des fichiers ouverts en lecture) ;
- Un fonctionnement stable même sur des ordinateurs anciens ;
- un noyau antivirus qui assure la détection et la neutralisation des logiciels malveillants qui n'ont pas encore été ajoutés à la base virale de Dr.Web, y compris ceux empaquetés par des packers inconnus.
- Une autoprotection fiable, qui résiste aux tentatives des virus de désactiver l'antivirus.

**Dr.Web ATM Shield est une seule solution qui tient compte des particularités des systèmes embarqués.**

### **Attention !**

**Voler de l'argent en utilisant des logiciels malveillants est un crime.**

Doctor Web offre une expertise des incidents informatiques viraux, ainsi qu'un examen psychologique des personnes (personnel) pour étudier l'implication / aide / dissimulation / promotion d'actes illégaux contre le client, le manque d'action ou la négligence.

## A propos de Doctor Web

Editeur russe, Doctor Web développe les solutions antivirus Dr.Web depuis 1992.

Doctor Web un des rares fournisseurs de solutions antivirus possédant ses propres technologies de détection et de traitement des programmes malveillants. Le système de protection antivirus Dr.Web résiste à tout type de menace.

Doctor Web est la première entreprise à avoir proposé sur le marché russe un modèle novateur d'antivirus en tant que service (Saas). Les certificats et prix d'Etat décernés aux produits Dr.Web, ainsi que l'étendue géographique des utilisateurs témoignent de la haute qualité des logiciels Dr.Web.

Les utilisateurs privés partout dans le monde, les petites et les moyennes entreprises, les établissements d'éducation et les instituts de recherche, les grandes entreprises du secteur énergétique, ainsi que les administrations, font confiance aux logiciels Dr.Web depuis plusieurs années.



© Doctor Web, 2003–2014

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

Phone: +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>