KASPERSKY lab

GUIDE DE SÉCURITÉ DESTINÉ AUX DAB ET AUX TERMINAUX DE POINTS DE VENTE

Garantir une sécurité efficace pour les systèmes de paiement critiques

www.kaspersky.fr

PROBLÈMES

Les systèmes embarqués posent des problèmes de sécurité spécifiques. Ils sont généralement dispersés géographiquement, peuvent être difficiles à gérer et sont rarement mis à jour. Comme ils gèrent des opérations impliquant de l'argent réel et des informations d'identification de carte de crédit, les distributeurs automatiques de billets et les terminaux de points de vente sont des cibles de choix pour les cybercriminels et demandent donc les niveaux les plus élevés de protection intelligente dédiée.

Les logiciels obsolètes représentent un problème très courant qui n'affecte pas uniquement les systèmes d'exploitation du grand public.
Il est bien connu que des satellites spatiaux toujours en fonctionnement utilisent du matériel et des logiciels datant de plusieurs dizaines d'années. Les systèmes de contrôle industriels connaissent, eux aussi, un problème lié aux systèmes d'exploitation très anciens et aux cycles de renouvellement très longs. Il en va de même pour les systèmes bancaires, et pas seulement en matière de terminaux. Les systèmes bancaires internes automatisés ne sont souvent pas mis à jour pendant des années. En termes de distributeurs automatiques de billets, 80 % des plus petites banques préfèrent attendre la prochaine fin de cycle (qui peut prendre de 5 à 10 ans, voire plus) pour acheter de nouvelles machines avec de nouveaux logiciels déjà installés, plutôt que d'effectuer des mises à jour vers les versions les plus récentes dès leur sortie.

Les familles Windows XP demeurent les systèmes d'exploitation les plus populaires pour les appareils DAB et PDV. La fin du support de ce système d'exploitation a affecté un grand nombre d'entreprises et d'organismes gouvernementaux. Les secteurs de la banque et du commerce, dans lesquels de nombreux distributeurs automatiques de billets du monde fonctionnent sous Windows XP Professional for Embedded Systems, ont été particulièrement touchés. Pourtant, le support de ce système a pris fin en avril 2014, en même temps que les versions grand public de Windows XP.

Le remplacement du logiciel des distributeurs automatiques de billets/terminaux de points de vente est un processus à la fois long, coûteux et fastidieux. En outre, le remplacement du logiciel implique bien souvent le changement d'équipements obsolètes, mais encore tout à fait fonctionnels.

PANORAMA DES CYBERMENACES

Les distributeurs automatiques de billets, qui se trouvent en dehors du périmètre physique de sécurité de la banque et qui contiennent de l'argent, et les systèmes de points de vente, qui capturent des données personnelles et des données bancaires vérifiées, occupent inévitablement une place élevée sur la liste des cibles des cybercriminels.

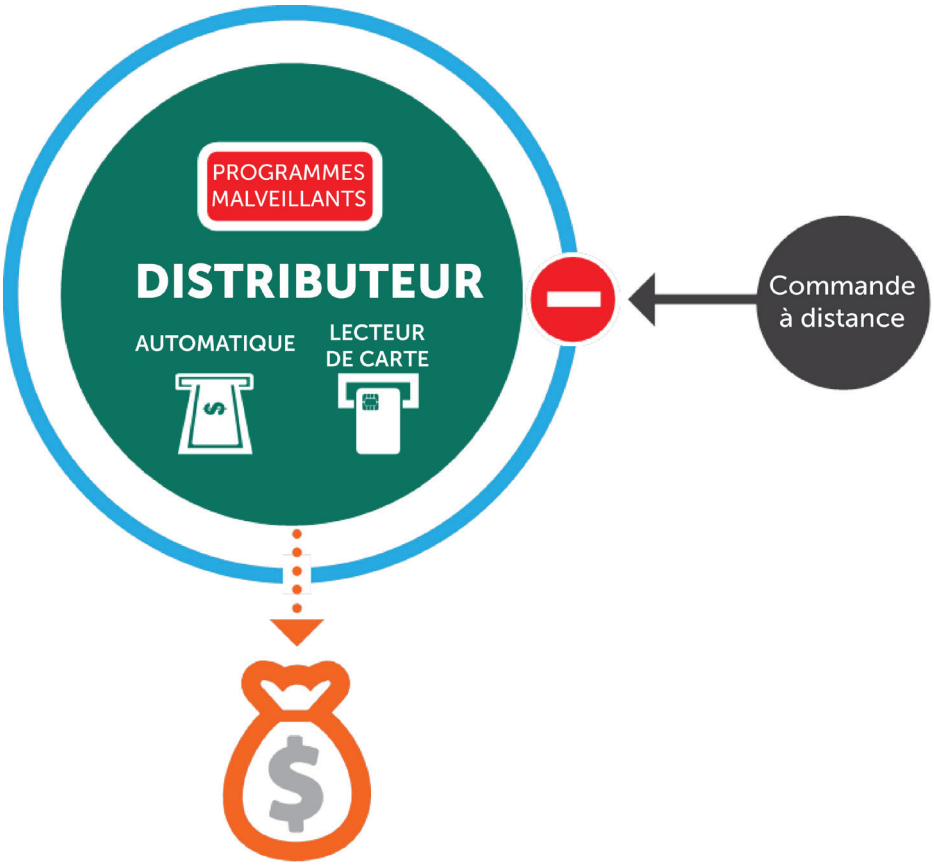
Depuis l'année 2009 qui a connu la première attaque sérieuse ciblant des distributeurs automatiques de billets avec les activités du programme malveillant Skimer, la quantité et la qualité des attaques a considérablement augmenté au fil des ans. En 2015, les attaques sur les systèmes de DAB et PDV ont atteint un autre niveau avec les programmes malveillants comme Ploutus, Tyupkin, Carbanak, CardStealer, vSkimmer, Chewbacca, POSeydon et FindPOS.

Une solution antivirus conventionnelle ne peut pas offrir une protection complète contre ces menaces, et les limites des systèmes des DAB et PDV (canaux faibles, matériel bas de gamme et logiciel obsolète) rendent son installation et son déploiement difficiles et souvent peu pratiques. En conséquence, ces virus continuent de pénétrer quotidiennement les systèmes des DAB et PDV de grands établissements financiers et de commerces.

Dans le même temps, un volume croissant de programmes malveillants des DAB et PDV extrêmement ciblés sont créés par des développeurs professionnels soutenus par le matériel et les systèmes les plus récents et les plus puissants.

Une simple attaque de distributeurs automatiques de billets est un moyen rapide et facile d'obtenir de l'argent comptant. Mais les infections des DAB peuvent aussi faire partie d'un scénario d'attaque plus vaste. Nous avons vu comment des attaques par menaces persistantes avancées, comme Carbanak en 2015, peuvent entraîner des pertes financières atteignant plus d'un milliard de dollars à travers le monde.

SCHÉMA D'ATTAQUE DES DISTRIBUTEURS AUTOMATIQUES DE BILLETS



Les terminaux de distributeurs automatiques de billets dispersés géographiquement sont parfaits pour introduire des infections causées par des programmes malveillants dans le cadre d'attaques ciblées, en particulier puisque les ports d'accès USB et les claviers sont facilement accessibles depuis un caisson de service système, sécurisé uniquement par un simple verrou situé à l'arrière du distributeur.

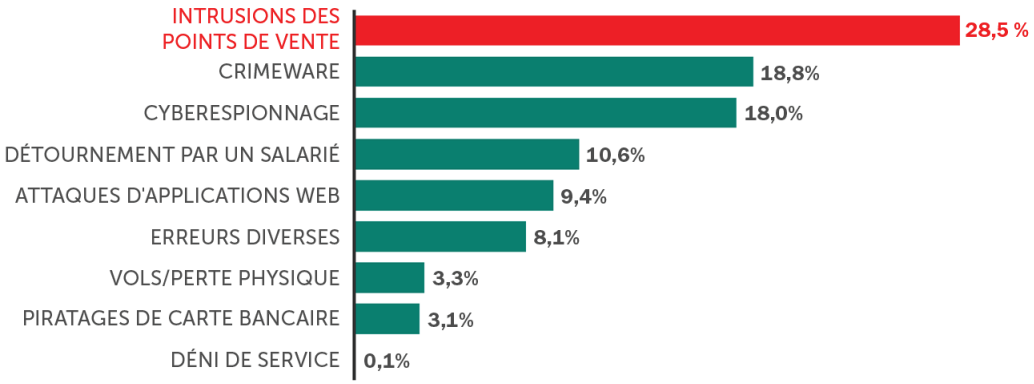
D'ailleurs, même le verrouillage peut représenter un problème. Il n'est en aucun cas inhabituel que les ingénieurs de service locaux installent un câble USB ou LAN/modem semi-permanent sortant du caisson de service du DAB, pour ne pas avoir à déverrouiller la porte à chaque fois. Malheureusement, il n'est pas pratique de désactiver les ports USB ou les lecteurs CD/DVD du caisson pour améliorer la sécurité. En effet, les ingénieurs doivent les utiliser régulièrement pour effectuer la maintenance de la machine.

À partir du moment où un programme malveillant s'est infiltré sur un système de DAB par une machine, il peut s'y cacher quelque temps, laissant le système fonctionner normalement pendant qu'il acquière des informations et se prépare. Puis, au moment venu, un code PIN ou une carte spécifique peut être utilisé pour déclencher le changement de logique du système, ce qui entraîne chaque DAB infecté à distribuer sur demande son contenu aux criminels.

MENACES BASÉES SUR LES TERMINAUX DE POINTS DE VENTE

FRÉQUENCE DES INCIDENTS DE SÉCURITÉ

CLASSIFICATION DES VIOLATIONS CONFIRMÉES DE DONNÉES

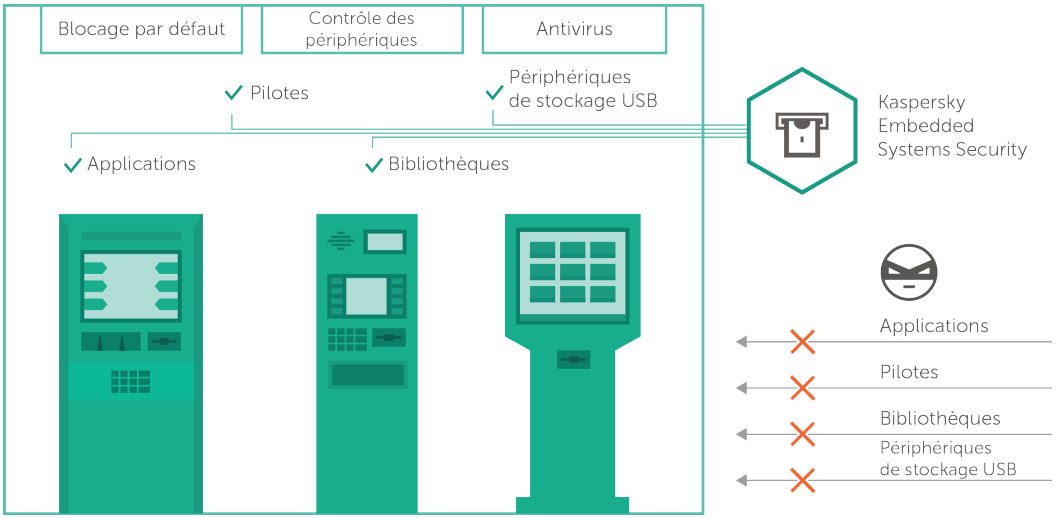


* VERISON : RAPPORT D'ENQUÊTES SUR LA VIOLATION DES DONNÉES, 2015

Un domaine particulier de vulnérabilité des systèmes de point de vente est le middleware dont ils dépendent. Ce middleware est souvent créé par de petits fournisseurs tiers ou en interne. Dans un souci de conception, les fonctionnalités peuvent passer avant la sécurité et, comme pour les distributeurs automatiques de billets, la facilité d'accès aux ports USB et aux lecteurs CD/DVD peut être considérée comme étant un avantage et non pas une faiblesse en matière de sécurité.

La plupart des systèmes PDV fonctionnent avec des cartes de crédit ou de débit et sont, comme les DAB, soumis à la norme PCI DSS. Ils utilisent tous, sans exception, les données personnelles des clients, dont la protection est la responsabilité du propriétaire des systèmes PDV. Enfin, ils sont tous connectés à un intranet, ce qui en fait un point d'entrée utile pour une attaque ciblée.

KASPERSKY EMBEDDED SYSTEMS SECURITY



Kaspersky Lab a conçu une solution de sécurité spécifiquement destinée aux entreprises gérant des systèmes des DAB et PDV et à l'environnement de menaces unique auquel elles font face. Cette solution répond à leurs exigences en matière de système d'exploitation, de canal et d'équipement tout en supportant totalement la famille logicielle Windows XP.

Kaspersky Embedded Systems Security atténue les risques de sécurité inhérents aux systèmes embarqués. La solution a été conçue spécifiquement pour les systèmes des DAB et PDV afin de protéger les surfaces d'attaque uniques à ces architectures, tout en respectant les équipements associés et les considérations en matière d'efficacité. Une console unique et intuitive vous donne le contrôle et la visibilité dont vous avez besoin pour gérer efficacement une sécurité multi-niveaux pour vos terminaux, vos systèmes clés et l'ensemble de votre infrastructure informatique.

La mise en œuvre du blocage par défaut pour les applications, pilotes et bibliothèques, renforcé par une fonctionnalité de contrôle des appareils, est la seule approche capable d'assurer la sécurité de systèmes techniquement « obsolètes », mais toujours en usage.

Kaspersky Embedded Systems Security propose un mode d'opération « blocage par défaut uniquement », où la configuration requise débute à 256 Mo de RAM et 50 Mo d'espace disque disponible, idéal pour les systèmes d'exploitation Windows XP utilisés sur du matériel bas de gamme. L'analyse à la demande est assurée par un module antivirus livré en option et alimenté par Kaspersky Security Network, qui est également assorti d'une fonctionnalité de gestion des correctifs selon les besoins.

Cette solution unique répond donc à trois objectifs clés :

- sécuriser efficacement les systèmes « difficiles à gérer »
- la conformité avec les exigences PCI DSS 5.1, 5.1.1, 5.2, 5.3 et 6.2
- permettre un étalement chronologique en douceur pour le remplacement des systèmes et des équipements obsolètes

Blocage par défaut

La plupart des solutions antivirus traditionnelles ne peuvent pas protéger totalement les équipements contre les menaces que représentent les programmes malveillants ciblés avancés auxquels le secteur est confronté. La fonction de blocage par défaut adopte une approche différente, plus fondamentale. Aucun fichier exécutable, pilote ou bibliothèque, en dehors de la protection logicielle, ne peut s'exécuter sur les terminaux de distributeurs automatiques de billets et de points de vente sans l'accord de l'administrateur de la sécurité informatique.

Contrôle des périphériques

Le contrôle des périphériques de Kaspersky Lab permet de surveiller les appareils tentant de se connecter physiquement aux systèmes, empêchant tout appareil non autorisé à accéder aux distributeurs automatiques de billets et aux unités de points de vente. Ainsi, ces points d'entrée vulnérables des systèmes, qui constituent souvent la première étape utilisée par les cybercriminels, sont bloqués.

Compatible Windows XP - Windows 10

Après 12 ans, le support de Windows XP Embedded a pris fin le 12 janvier 2016 et pour Windows Embedded for Point of Service, le 12 avril 2016. Il n'y a plus de mises à jour de sécurité ou d'assistance technique pour le système d'exploitation Windows XP. Kaspersky Embedded Systems Security fournit un support intégral (100 %) de la gamme Windows XP.

Conçu pour les systèmes embarqués

Kaspersky Embedded Systems Security doit garantir une efficacité optimale sur les systèmes bas de gamme, caractéristiques du matériel de la plupart des distributeurs automatiques de billets et des terminaux de points de vente. Les prérequis débutent à seulement 256 Mo de RAM pour la famille Windows XP, avec environ 50 Mo d'espace disque nécessaire sur le disque dur. Lors du fonctionnement en mode « à la demande », le module antivirus installé séparément est conçu pour n'utiliser les ressources du système que lors des scans manuels ou planifiés.

Antivirus et Kaspersky Security Network

Les réglementations de la norme PCI DSS précisent qu'un antivirus doit être installé et mis à jour régulièrement sur tous les systèmes qui assurent l'interface avec les cartes de crédit ou de débit. Kaspersky Embedded Systems Security offre une protection antivirus efficace, combinée aux mises à jour automatiques ou manuelles régulières des signatures, comme exigé. Comme plus de la moitié de tous les programmes malveillants détectés sur les systèmes des distributeurs automatiques de billets et des terminaux de points de vente sont entrés par le biais de failles « zero-day »/« zero-second », Kaspersky Lab recommande également d'appliquer une sécurité intelligente grâce à la technologie Kaspersky Security Network afin de prévenir et d'atténuer les risques de sécurité liés aux failles et de réduire le délai de réaction.

CONFORMITÉ AUX NORMES PCI DSS

La fonctionnalité Kaspersky Security for Embedded Systems respecte et surpasse toutes les normes en matière de sécurité répertoriées dans les sous-sections de la norme PCI DSS v3.1 :

5.1 : Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).

5.1.1 : S'assurer que tous les programmes anti-virus sont capables de détecter et d'éliminer tous les types de logiciel malveillant connus, et d'assurer une protection efficace.

5.2 : S'assurer que tous les mécanismes antivirus sont maintenus à jour, effectuent régulièrement des analyses et génèrent des journaux d'audit qui sont conservés selon la condition 10.7 de la norme PCI DSS.

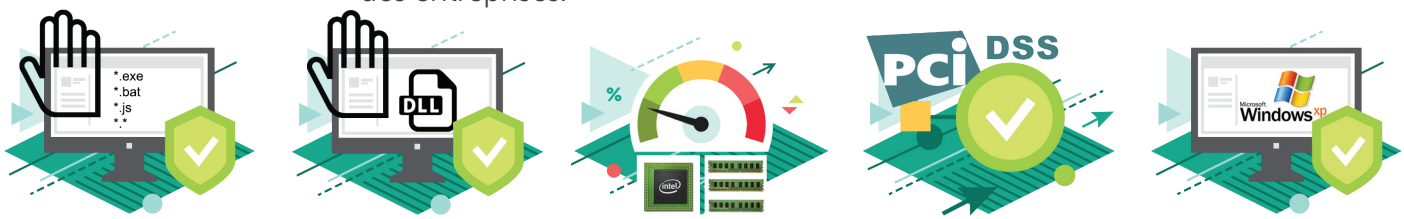
5.3 : S'assurer que les mécanismes anti-virus fonctionnent de manière active et ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.

6.2 : S'assurer que tous les logiciels et les composants du système sont protégés de vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation.

AU-DELÀ DE L'ANTIVIRUS

La norme sur la sécurité des données du secteur des cartes de paiement (Payment Card Industry Data Security Standard, PCI DSS) réglemente de nombreuses exigences techniques et de nombreux paramètres pour les systèmes basés sur les données de carte de crédit. Cependant, les réglementations en matière de sécurité pour les distributeurs automatiques de billets et les terminaux de points de vente semblent ne couvrir que la sécurité basée sur l'antivirus. Comme mentionné précédemment et amplement démontré lors des dernières attaques, une approche purement antivirus est d'une efficacité limitée contre les menaces rencontrées actuellement par les distributeurs automatiques de billets/terminaux de points de vente. Il est temps maintenant d'appliquer à vos systèmes embarqués les plus stratégiques le contrôle des périphériques et le blocage des applications, qui ont déjà fait leurs preuves dans d'autres contextes de sécurité.

Pour en savoir plus sur la protection efficace de vos terminaux de systèmes de paiement critiques, contactez l'équipe commerciale Kaspersky Lab chargée des entreprises.




Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/
Kaspersky

Kaspersky Lab, Moscou, Russie
www.kaspersky.fr

Tout savoir sur la sécurité sur
Internet : www.securelist.fr

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

KASPERSKY lab