KASPERSKY lab

Kaspersky Embedded Systems Security – Protéger les DAB

www.kaspersky.fr
#truecybersecurity

Kaspersky Embedded Systems Security – Protéger les DAB

De gros problèmes pour de petites boîtes

Les DAB ont toujours attiré l'attention des malfaiteurs. Pour mettre la main sur le contenu de ces machines, les malfaiteurs ont eu recours (et parfois, continuent d'avoir recours) à des mesures radicales : l'utilisation de perceuses électriques, de scies circulaires, de chalumeaux, d'explosifs et même parfois d'un véhicule pour les remorquer.

Par la suite, ils ont utilisé différents skimmers, des appareils spécialement conçus pour dérober les coordonnées bancaires dont un DAB a besoin pour fonctionner. Cependant, avec l'introduction de la norme internationale « EMV » (Europay, MasterCard, VISA), qui définit un certain nombre d'exigences en matière d'interaction entre une carte bancaire et un appareil de paiement, la sécurité des opérations financières effectuées sur les DAB a fortement augmenté. Le volume des clonages de cartes bancaires utilisées dans les DAB a donc considérablement baissé.

Cependant, les malfaiteurs n'ont pas abandonné : au lieu de tentatives isolées de cibler les DAB à l'aide d'outils électriques ou de câbles métalliques, ils ont commencé à utiliser des logiciels malveillants spécialement conçus à cet effet. Ils n'ont plus besoin d'explosifs ou d'une carte « en plastique blanc » (une carte spécialement préparée avec des données provenant d'une carte de paiement volée). Il leur suffit d'infecter un DAB avec un cheval de Troie qui leur permet de retirer tous les billets du DAB dès qu'ils en ont besoin. En plus de voler de l'argent, les malfaiteurs peuvent également modifier le fonctionnement de la machine et lancer une attaque DoS (Denial of Service, déni de service) qui entraînera des pertes financières pour la banque propriétaire du DAB.

Au fil des années, les établissements financiers ont observé un certain nombre d'échantillons de logiciels malveillants ciblant les DAB. Par exemple, le premier programme malveillant ciblant les DAB (Backdoor.Win32.Skimmer) a été détecté par Kaspersky Lab en 2009 et est toujours présent sur certaines machines. Ce cheval de Troie dérobe les données de carte bancaire de l'utilisateur et peut également distribuer des billets sans que le titulaire du compte n'en ait connaissance.

Trojan-Spy.Win32.SPSniffer et Chupa Cabra constituent deux autres exemples intéressants. Ce cheval de Troie a été détecté pour la première fois en 2010 par les experts Kaspersky Lab au Brésil, et fonctionne sur tous les types de DAB en interceptant des données des distributeurs afin de lire les informations des cartes.

Nous avons accumulé suffisamment d'exemples de ces types de chevaux de Troie pour en analyser les échantillons les plus utilisés et définir les mesures et technologies requises pour la protection des DAB.

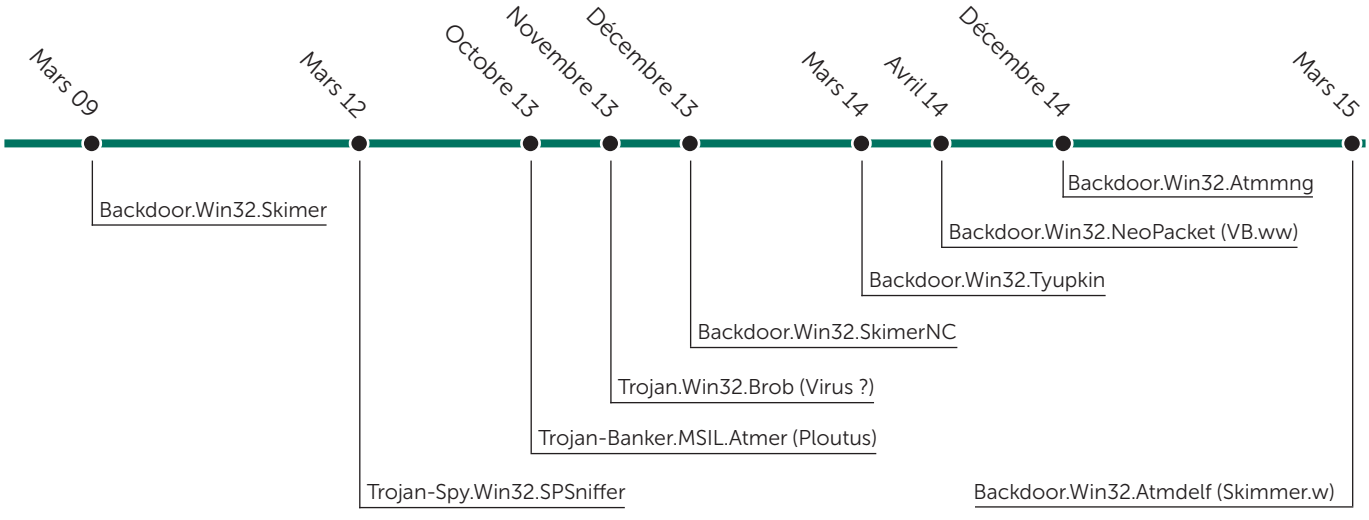


Figure 1 : Calendrier de la détection des programmes malveillants des DAB

Backdoor.MSIL.Tyupkin

En mars 2014, le monde découvrait un logiciel malveillant installé sur les DAB, qui permettait aux malfaiteurs de retirer d'énormes sommes d'argent. Pour le malfaiteur, il suffisait de se rendre sur un DAB infecté et de saisir un code sur le clavier pour que la machine distribue tout son contenu.

Avant d'analyser le fonctionnement de ce code malveillant et la manière dont il a atterri sur les DAB, il est important de comprendre que chaque DAB est conçu pour exécuter certaines tâches spécifiques. Ceci signifie que les DAB sont confrontés au même type de menaces que les stations de travail et les serveurs traditionnels, et que les systèmes d'exploitation lancés sur les ordinateurs des DAB peuvent contenir les mêmes vulnérabilités que les ordinateurs de bureau et les serveurs.

Selon les experts Kaspersky Lab, le programme malveillant Tyupkin (Backdoor.Win32.Tyupkin) était installé sur les DAB à l'aide d'un CD de démarrage utilisé par un malfaiteur ayant un accès direct à l'ordinateur du DAB.

Après avoir pénétré dans le système d'exploitation du DAB, le programme malveillant restait sur la machine infectée, ce qui assurait aux malfaiteurs l'accès à son contenu.

Une fois sur l'appareil, le cheval de Troie désactivait immédiatement la solution de protection d'un fournisseur spécifique installée sur le DAB en retirant ses composants logiciels, lançait une boucle infinie en attendant une action de l'utilisateur et, afin de ne pas être repéré, acceptait les commandes uniquement les dimanches et lundis soir. Armés des commandes et du code spécifique acceptés par le cheval de Troie pour exclure toute interaction avec un utilisateur aléatoire, les malfaiteurs pouvaient accéder au contenu des cassettes du DAB et retirer les billets.

Cependant, Tyupkin n'était pas la seule menace pesant sur les DAB rencontrée par les experts Kaspersky Lab.

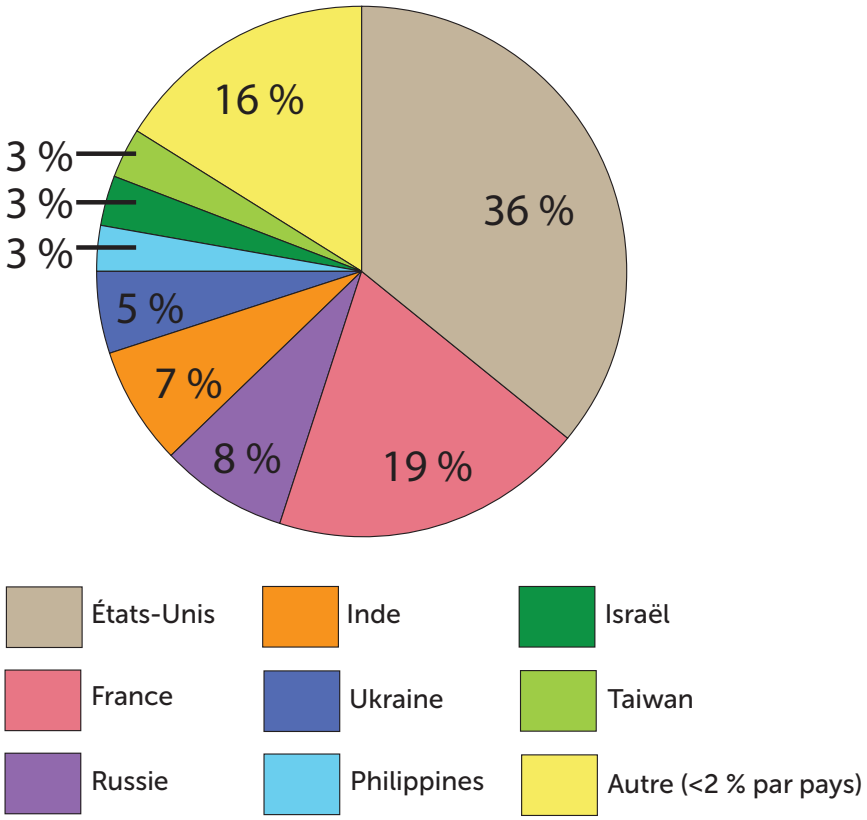


Figure 2 : Nombre d'échantillons Tyupkin par pays (selon les statistiques VirusTotal)

Carte des cibles de Carbanak

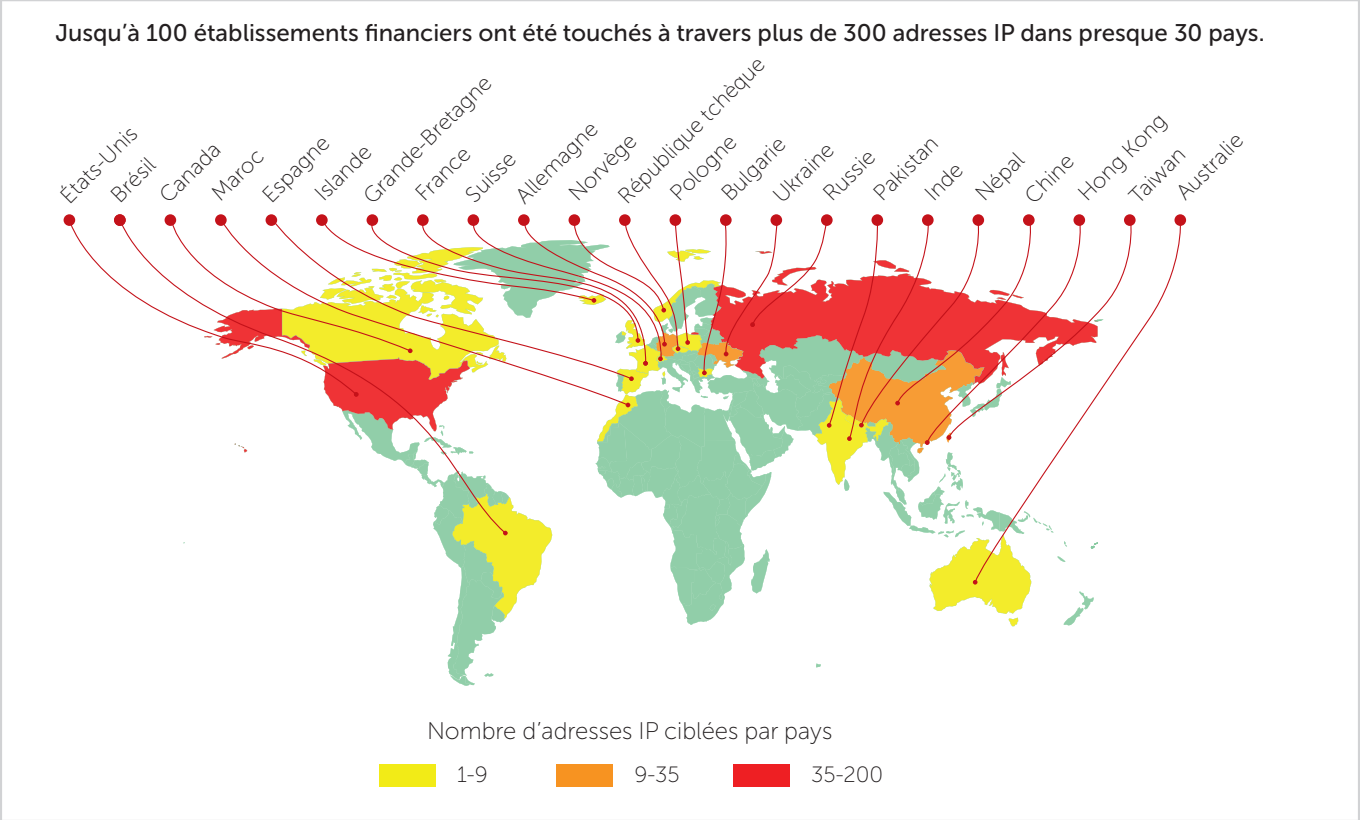


Figure 3 : Infection de Carbanak par pays

Carbanak

Au printemps 2014, Kaspersky Lab a participé à une enquête judiciaire suite à la distribution de billets par les DAB d'une banque sans qu'aucune interaction physique n'ait eu lieu entre le destinataire légitime et le DAB. C'est ainsi qu'ont démarré l'enquête sur la campagne Carbanak et la recherche sur le programme malveillant éponyme.

Carbanak est un backdoor basé sur le code Carberp. Il est conçu à des fins d'espionnage, de collecte des données et d'accès à distance à l'ordinateur infecté. Les malfaiteurs accédaient à une machine sur le réseau de la banque, puis exploraient le réseau pour y trouver le moyen de propager l'infection vers les systèmes essentiels : traitement, comptabilité et DAB. Ils le faisaient manuellement en essayant de pirater les ordinateurs ciblés (par exemple les machines de l'administrateur) et en utilisant des outils susceptibles de répandre l'infection sur les autres ordinateurs du réseau. En d'autres termes, après avoir accédé au réseau, ils passaient d'un ordinateur à l'autre jusqu'à ce qu'ils trouvent un objet qui les intéresse. Le choix des objets variait en fonction des attaques, mais le résultat était toujours le même : les malfaiteurs volaient de l'argent à un établissement financier et les DAB étaient l'un des premiers canaux de retrait.

Si les malfaiteurs parvenaient à pénétrer dans des ordinateurs ayant accès au réseau de DAB interne ou si la banque elle-même accédait à distance à ses DAB, les fraudeurs utilisaient ces fonctionnalités pour retirer de l'argent. Ils n'avaient même pas besoin d'outils spéciaux pour infecter les logiciels des DAB : les malfaiteurs utilisaient une série d'outils standard conçus pour contrôler et tester légitimement les équipements DAB.

Les solutions informatiques installées sur les DAB sont, dans la plupart des cas, des programmes agents qui reçoivent des commandes de la part de stations de travail spéciales sur le réseau interne de la banque et auxquelles ils envoient des données. Par exemple, ces agents peuvent faire ce qui suit :

- Surveiller les événements ayant lieu dans le DAB.
- Diffuser les programmes dans tous les DAB de la banque.

- Télécharger les fichiers des DAB vers un serveur dédié au sein de la banque.
- Fournir un accès à distance aux DAB.

Ces agents sont utilisés pour permettre aux employés de la banque d'administrer et de configurer les DAB à distance, et figurent par conséquent le plus souvent sur la « liste blanche » de logiciels d'un DAB. C'est pourquoi, comme l'ont montré les attaques Carbanak, ils intéressent tout particulièrement les malfaiteurs qui parviennent à accéder au réseau interne d'une banque.

La sécurité des systèmes embarqués

Un système embarqué est un ordinateur spécialisé qui se trouve directement sur l'appareil qu'il gère. S'agissant des distributeurs automatiques, c'est un ordinateur de contrôle embarqué dans le DAB. Ces ordinateurs exécutent des versions spécifiques d'un système d'exploitation telles que le système Embedded Windows. Bien qu'un nombre strictement limité de logiciels soient installés dans ce système d'exploitation pour le fonctionnement du DAB, le système peut présenter des vulnérabilités nécessitant des moyens de protection supplémentaires, au même titre que ses versions serveur et de bureau.

Les incidents Tyupkin décrits plus haut montrent que les pirates n'ont eu aucune difficulté à copier le programme malveillant d'un CD-ROM de démarrage vers un DAB et à exécuter ses fichiers. À ce stade, nous constatons déjà que les recommandations en matière de protection physique des DAB n'ont pas été suivies, ce qui a donné aux cybercriminels la possibilité d'utiliser le CD de démarrage. Cependant, le problème n'est pas uniquement la vulnérabilité physique de l'appareil, mais également le fait que les malfaiteurs aient pu exécuter un code malveillant arbitraire. Après avoir lancé ce code malveillant, les fraudeurs ont pu accéder aux cassettes remplies d'argent du DAB.

Plan d'attaque Tyupkin

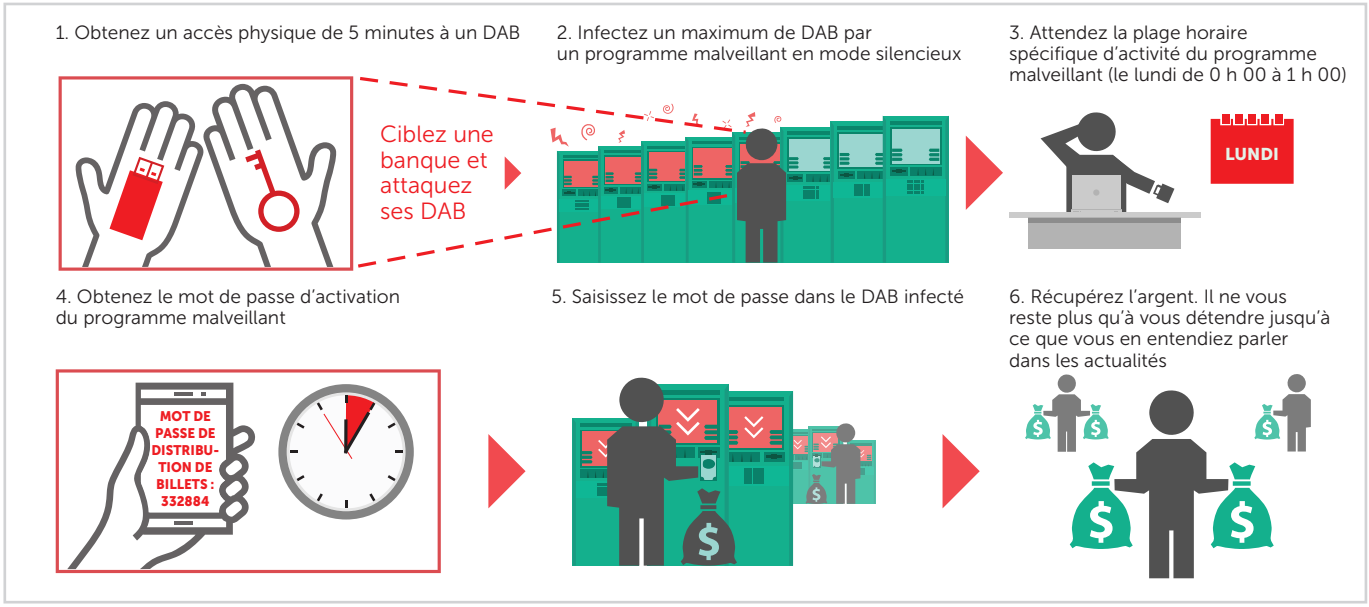


Figure 4 : Le programme malveillant de DAB « Tyupkin » force les DAB à basculer en mode maintenance et les fait « cracher » des billets

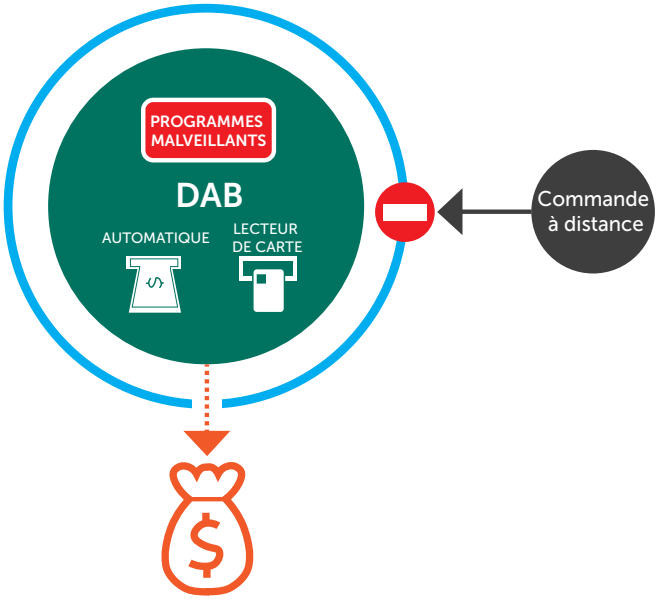


Figure 5 : Même si le DAB ne comprend pas d'outils d'accès à distance, les malfaiteurs peuvent utiliser des programmes malveillants pour retirer de l'argent illégalement ou dérober des données de paiement

L'approche « blocage par défaut »

Le monde des serveurs et stations de travail traditionnels a adopté depuis longtemps l'approche « blocage par défaut » ainsi que la technologie de « liste blanche » correspondante, qui autorise l'utilisation de logiciels d'entreprise uniquement sur les ordinateurs du bureau. Cependant, les solutions logicielles traditionnelles qui utilisent ces technologies et s'exécutent sur des stations de travail et serveurs ne sont pas conçues pour les systèmes embarqués qui, dans la plupart des cas, fonctionnent sur des matériels dotés de ressources de calcul très faibles. Ceci impose certaines restrictions à l'utilisation des solutions de sécurité existantes, qui nécessitent des ressources de calcul non disponibles sur les ordinateurs embarqués dans les DAB.

Les experts Kaspersky Lab ont développé la solution spécialisée Kaspersky Embedded Systems Security afin de protéger les systèmes embarqués. Cette solution tient compte des caractéristiques spécifiques de ces appareils et contient une technologie de « blocage par défaut » permettant de lutter contre les cybermenaces ciblant les systèmes d'exploitation embarqués. Ceci signifie que toutes les applications du système d'exploitation du DAB sont exécutées conformément au scénario suivant :

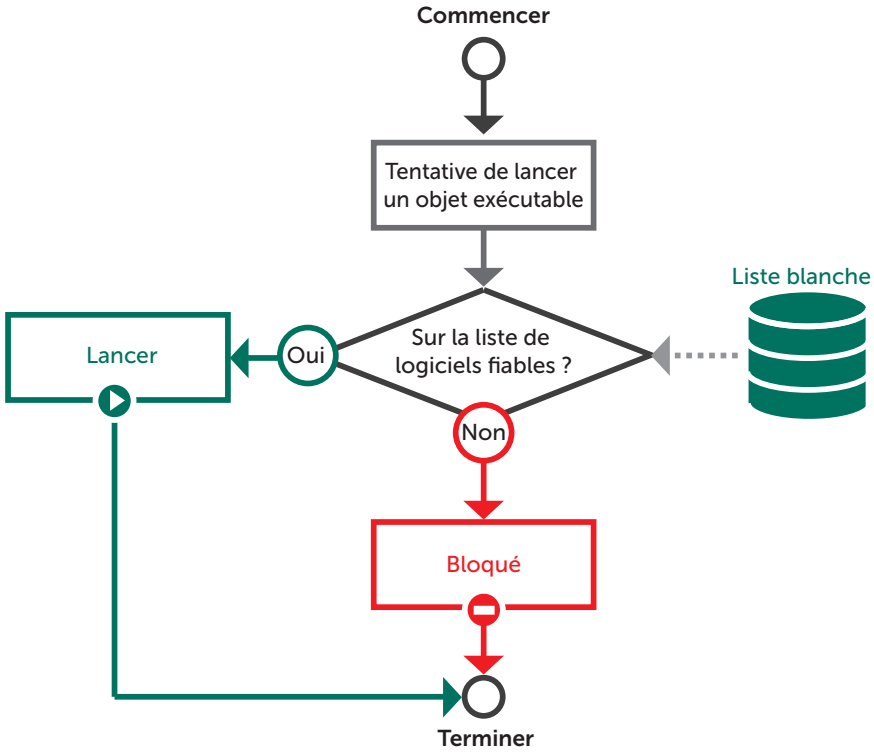
- Le système d'exploitation initie le lancement d'une application, d'un script ou d'une bibliothèque.
- Le système de sécurité du produit vérifie si l'application, la bibliothèque ou le script est fiable, en utilisant une liste blanche des applications fiables et de leurs composants.
- Si l'objet est reconnu comme fiable, il peut s'exécuter. Sinon, il est bloqué.

La technologie de « blocage par défaut » crée un environnement logiciel dans le système d'exploitation du DAB dans lequel seules les applications requises pour exécuter des tâches DAB sont autorisées. Par conséquent les tentatives, par des cybercriminels, d'exécuter des codes arbitraires dans un système d'exploitation du DAB protégé par la technologie de « blocage par défaut » s'avéreront infructueuses.

Éliminer les téléchargements non autorisés

Cependant, dans le cas de Tyupkin, les cybercriminels ont mis en œuvre une approche non-triviale d'exécution de codes malveillants en procédant au téléchargement à partir d'un CD-ROM de démarrage spécialisé. Ils ont ainsi eu accès aux répertoires du système d'exploitation du DAB et ont manipulé les fichiers. Ceci leur a permis de télécharger des codes malveillants et de recevoir tous les privilèges nécessaires pour assurer leur fonctionnement à l'intérieur du système d'exploitation.

Afin de protéger les DAB de ce type de menace, il est nécessaire d'éliminer la possibilité de téléchargements non autorisés à partir de médias externes susceptibles de contenir des codes malveillants ou visant à désactiver une solution de protection installée. Cette procédure peut être mise en œuvre en réglant l'ordre de chargement correct dans le BIOS (le téléchargement du système d'exploitation du DAB par le disque dur doit avoir lieu en premier) et en protégeant les paramètres BIOS par un mot de passe. Le chiffrement intégral du disque dur (FDE) à partir duquel le système d'exploitation du DAB est téléchargé constitue une autre approche en matière de protection des DAB. Lorsque la technologie FDE, qui est mise en œuvre dans Kaspersky Endpoint Security for Windows, est déployée sur un DAB, elle peut bloquer les tentatives, par les cybercriminels, d'accéder à l'appareil de saisie du DAB afin de modifier les fichiers de système d'exploitation, de manipuler le système de fichiers du DAB ou de lancer des codes malveillants lors de l'exécution du système d'exploitation. Cependant, il convient de souligner que l'utilisation de ce mécanisme comprend certains risques en termes d'intégrité et de disponibilité des appareils ; ainsi, l'utilisation du FDE pourrait s'avérer inadaptée dans certains cas.



Cependant, comme l'ont montré les attaques Carbanak, même les outils d'accès à distance et de surveillance spécialisés et non malveillants, qui figurent sur la liste blanche par défaut, pourraient poser problème s'ils sont installés sur un DAB et si les cybercriminels parviennent à pénétrer dans les ordinateurs ayant accès au réseau de DAB interne.

Surveiller pour protéger

Pour lutter contre les menaces dans le cadre desquelles les cybercriminels utilisent les outils standards installés sur les DAB, les responsables de la sécurité informatique doivent mettre en œuvre les mesures proactives suivantes :

- Éliminer la possibilité d'accéder aux DAB à distance.
- Empêcher toute manipulation essentielle des équipements (s'il n'est pas possible de bloquer l'accès à distance au DAB, il est nécessaire, au moins, d'exclure du réseau d'entreprise les stations de travail contrôlant des DAB).
- Utiliser un seul outil pour surveiller et assurer la sécurité du DAB.

Dans notre cas, cet outil de surveillance est le Kaspersky Security Center, qui fait partie de Kaspersky Embedded Systems Security. Il collecte des informations concernant le statut de chaque DAB et permet également de générer des rapports à partir d'outils de surveillance tiers installés sur les DAB. Les administrateurs des DAB peuvent donc analyser le statut de chaque appareil dans le Kaspersky Security Center tout bloquant l'accès aux « portes d'entrée » supplémentaires (outils d'accès à distance) aux malfaiteurs.

Assurer la sécurité des DAB ; bilan

Le système d'exploitation des DAB est une version spécifique du système d'exploitation des stations de travail traditionnelles et comporte les mêmes risques. Autrement dit, même si le DAB ne subit pas d'attaque ciblée impliquant un cheval de Troie spécialement développé à cette fin, il pourra toujours être infecté par un programme malveillant de bureau standard, lequel pourra également perturber le fonctionnement de la machine et entraîner des pertes financières importantes. Ainsi, la solution de sécurité Kaspersky Lab pour les systèmes embarqués intègre des technologies antivirus conçues pour assurer une protection non seulement contre les menaces spécifiques aux DAB, mais également contre toutes les autres formes de programmes malveillants susceptibles d'être présents dans le système d'exploitation et de perturber les services.

Les établissements financiers doivent être davantage vigilants en ce qui concerne la protection de leurs distributeurs et tenir compte de la sécurité de leurs composants matériels comme de leurs systèmes d'exploitation des DAB, ainsi que de l'infrastructure du réseau au sens large. Pour ce faire, ils peuvent utiliser des outils de protection employés depuis longtemps sur les réseaux d'entreprise, ainsi que des solutions de sécurité spécialisées pour les systèmes embarqués. Cependant, si un incident a lieu, il est important d'intervenir rapidement et de collaborer activement avec les organismes chargés de l'application de la loi et les sociétés spécialisées dans la sécurité informatique.

Un monde d'expertise en technologies Kaspersky Lab

L'efficacité des produits Kaspersky Lab est régulièrement prouvée par les résultats de tests indépendants. En 2016, la société est arrivée en tête du top 3 des fabricants de solutions de sécurité. Selon les résultats de 78 tests différents réalisés par des entreprises réputées dans plusieurs pays, les solutions Kaspersky Lab figurent dans le top 3 de 90 % des tests et arrivent en tête à 60 occasions. C'est une preuve indéniable que Kaspersky Lab fournit la meilleure protection du secteur.

À propos de Kaspersky Lab

Kaspersky Lab est une entreprise mondiale de cybersécurité fondée en 1997. Kaspersky Lab s'appuie sur sa veille stratégique et son expertise en matière de sécurité informatique pour développer des solutions de sécurité destinées aux entreprises, aux infrastructures critiques, aux gouvernements et aux utilisateurs du monde entier. Le portefeuille de solutions de sécurité inclut la protection des postes de travail, classée parmi les leaders. De nombreux services, et des solutions de sécurité spécifiques, permettent également de lutter contre les cybermenaces sophistiquées et évolutives. Plus de 400 millions d'utilisateurs sont protégés par les technologies de Kaspersky Lab et nous aidons 270 000 clients professionnels à protéger ce qui compte le plus à leurs yeux.

Plus d'informations sur : https://www.kaspersky.fr/enterprise-security

Solutions de sécurité Kaspersky Lab
pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.fr