Une nouvelle menace plane sur les distributeurs automatiques de billets

	Une nouvelle menace plane sur les distributeurs automatiques de billets

Des chercheurs en sécurité informatique ont découvert une faiblesse des DAB, difficilement détectable à ce jour.

Les distributeurs automatiques de billets restent une cible appréciée des pirates informatiques. Selon une étude publiée par Kaspersky , une entreprise spécialisée en cybersécurité, et relayée par 01Net , les « DAB » seraient vulnérables à une attaque informatique perfectionnée et surtout, discrète. Cette attaque a été détectée 10 fois en France, rapporte Kaspersky. C'est le deuxième pays à être autant ciblé après les Etats-Unis.
La méthode est assez ingénieuse. « Alors que les virus que l'on connaît aujourd'hui écrivent des fichiers sur le disque dur du DAB, cette nouvelle génération d'attaques va s'en prendre à la mémoire vive, ce qui ne laisse aucune trace », décrit Daniel Fages, directeur technique de Stormshield, une entreprise française spécialisée, aux « Echos ». Une fois introduit dans le système, qui est peu ou prou un ordinateur, l'attaquant va pouvoir prendre le contrôle de la machine à distance, à n'importe quel moment. L'attaque a un nom : « fileless malware », ou malware « sans fichier », en bon français.

Les Etats-Unis sont particulièrement touchés par le phénomène – Kaspersky

A partir de là, tout est possible. « L'attaquant peut faire sortir des billets comme il l'entend, ou bien capturer les données des utilisateurs qui retirent des billets dans le DAB infecté », décrit Daniel Fages.

Les DAB, pas réellement protégés

Cette vulnérabilité est d'autant plus importante que les distributeurs ne sont que très rarement mis à jour aujourd'hui. Si certaines banques disposent de protection contre les virus « classiques », très souvent, elles s'en contentent. « Tant que ça marche, on ne touche pas », résume Daniel Fages.
Difficulté supplémentaire : les DAB sont produits sur un mode industriel. Une faille telle que celle-ci peut donc fonctionner sur de très nombreux appareils.

Une attaque difficile à réaliser

Néanmoins, une telle attaque n'est pas facile à réaliser. Pour infiltrer la mémoire vive du distributeur, il faut d'abord avoir infecté le réseau qui relie les DAB d'une même banque entre eux. Ce réseau, souvent interne, n'est pas directement exposé à Internet et donc à une attaque.
« Les attaquants capables d'une telle manoeuvre ont des moyens et de très bonnes connaissances techniques », estime Daniel Fages.

Une sécurité : protéger son code PIN

Qui plus est, si les attaquants décident de s'en prendre aux données des …[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Une nouvelle menace plane sur les distributeurs automatiques de billets, Banque –

Assurances