The Hotel **Hijackers**

pandasecurity.com

panda

Les pirates des hôtels

Apres plus de 25 années passées dans la sécurité Informatique, il y a une chose dont nous sommes sûr : La première motivation d'un cyber délinquant est toujours l'argent.

C'est la raison pour laquelle les pirates utilisent des chevaux de Troie pour obtenir les informations confidentielles se trouvant dans nos ordinateurs et terminaux mobiles.

Cryptolocker en est un exemple récent : **une attaque très répandue qui utilise un logiciel d'extorsion (Ransomware) pour crypter les données importantes** puis exige de la victime le paiement d'une rançon pour récupérer les données compromises.

Au fil du temps nous avons observé les malwares "Traditionnels" autant que les nouvelles attaques qui sont conçues spécifiquement pour chaque cible et comment les entreprises prennent en compte ces attaques..

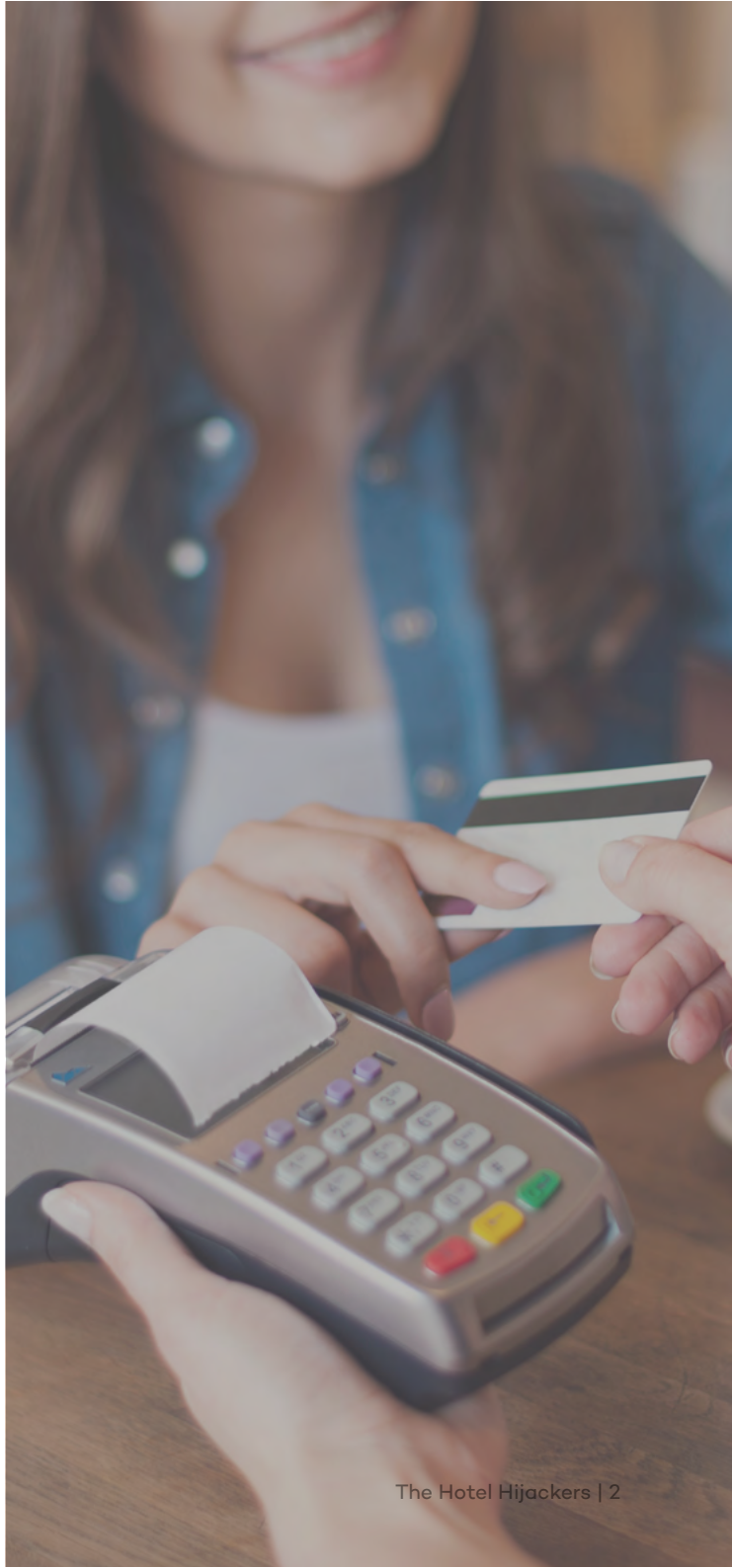
Tout récemment, ces cyber-délinquants s'en sont pris aux chaines hôtelières.

Pourquoi les hôtels?

Les cybercriminels considèrent en effet les hôtels comme un marché particulièrement juteux.

Quand ils s'attaquent à un hôtel, les pirates réfléchissent à la façon dont ils pourront prendre dans leurs filets les milliers de chambres utilisées par des millions de client et qui génèrent des millions de dollars de recettes.

De la réservation de la chambre aux paiements réalisés dans les boutiques et les restaurants, les chaines hôtelières sont dotées de réseaux complexes qui contiennent d'énormes quantités de données privées souvent sensibles qui ne demandent qu'a être subtilisées. Si vous avez séjourné récemment dans un hôtel, il se peut que vous éprouviez le besoin de vérifier en détail vos relevés de cartes de crédit...



Les détails de l'affaire

L"année 2015 a marqué un tournant pour ce secteur d'activité car , **la plupart des hôtels, quelque soit leur taille ont été victimes de cyber-attaques dans le courant de cette année**.

Les cybercriminels ont aussi les yeux rivés sur les entreprises qui délivrent des prestations aux chaines hôtelières.

White Lodging

White Lodging gère un nombre d'hôtels bien connus comme Hilton, Marriott, Hyatt, Sheraton, et Westin. Bien qu'il s'agisse davantage d'une société de gestion d'hôtels que d'une chaine d'hôtels, elle a néanmoins été l'objet d'une importante cyber-attaque qui a été rendu publique en 2014. En 2013, **les données de cartes de crédit et de retrait de clients de 14 hôtels ont été compromises**.

Deux ans plus tard, une autre attaque a frappé dix hôtels, dont certains avaient déjà été victimes de la première attaque. Les pirates voulaient subtiliser davantage d'information des données bancaires des clients (nom, cryptogramme, date d'expiration). Selon White Lodging, le processus de cette attaque était différent de la première tentative de 2013.

24 hôtels affectés

Mandarin Oriental

La luxueuse chaine Mandarin Oriental a également été attaquée en mars 2015. **Le malware a infecté les terminaux POS** (points de vente) de certains hôtels du groupe situés en Europe et aux Etats Unis.

Le malware était spécialement conçus et orienté vers les systèmes des terminaux de paiement afin de voler les données des cartes bancaires.

Des milliers de cartes de crédit compromises

Trump Hotels

Sept de leurs établissements ont été attaqués de mai 2014 à juin 2015.

Comme ils l'ont reconnus, **des données provenant de cartes bancaires de clients ont été dérobé de terminaux de paiement et d'ordinateurs** situés dans leurs restaurants, boutiques de souvenirs et autres commerces.

Il a suffit d'une seule année aux cybercriminels pour subtiliser des tonnes d'information confidentielles.

Des dizaines de stations de travail et de terminaux de paiements infectés

Hard Rock Las Vegas

Une attaque a infecté les terminaux de paiement de certains de leurs restaurants, bars et boutiques mais les terminaux POS de l'hôtel et du casino n'ont pas été affecté.

Pendant toute la durée de la période entre septembre 2014 et avril 2015, le Hard Rock Las Vegas a du faire face à une série d'attaques **pour un bilan de 173 000 cartes bancaires piratées** dans les restaurants, bars et boutiques de l'hotel.

Mais ce ne fut pas le seul Hôtel-Casino affecté. L' établissement FireKeepers, situé à Battle Creek, fut également touché en 2015.

173,000 cartes bancaires dérobées.

Hilton Worldwide

En novembre 2015, le groupe Hilton Worldwide a diffusé un communiqué de presse ou il reconnaissait avoir été victime d'une cyber-attaque.

Peu d'informations ont été divulguées sur la nature précise de l'attaque mais il s'avère que **les données complètes des cartes bancaires de plusieurs clients ont été dérobées**.

Par chance, les PIN et autres codes personnels n'ont pas été compromis.

Accès à des informations confidentielles

Starwood

Approximativement à la même date que pour Hilton Worldwide, la chaine Starwood annonça qu'elle avait aussi été victime d'une cyber-attaque.

105 hôtels de la chaine furent attaqués (Sheraton, St. Regis, Westin, W, etc.), ce qui en fait **la plus grosse attaque du genre dans le secteur hôtelier sur la période**.

Starwood publia une liste des hôtels dont les caisses enregistreuses et terminaux de paiement avaient été infectés par le code malveillant.

105 hôtels affectés

Hyatt

Le record de l'attaque Starwood fut de courte durée. Il fut en effet suivi par ce qui s'avère encore aujourd'hui comme la plus importante cyber-attaque ayant affecté le secteur hôtelier.

La chaine d'hôtels Hyatt confirma dans un communiqué que, **suite au piratage des terminaux de paiement (POS) de 249 de leurs hôtels dans 54 pays**, l' ensemble des informations des cartes de crédit de leurs clients avaient été dérobés entre juillet et septembre 2015.

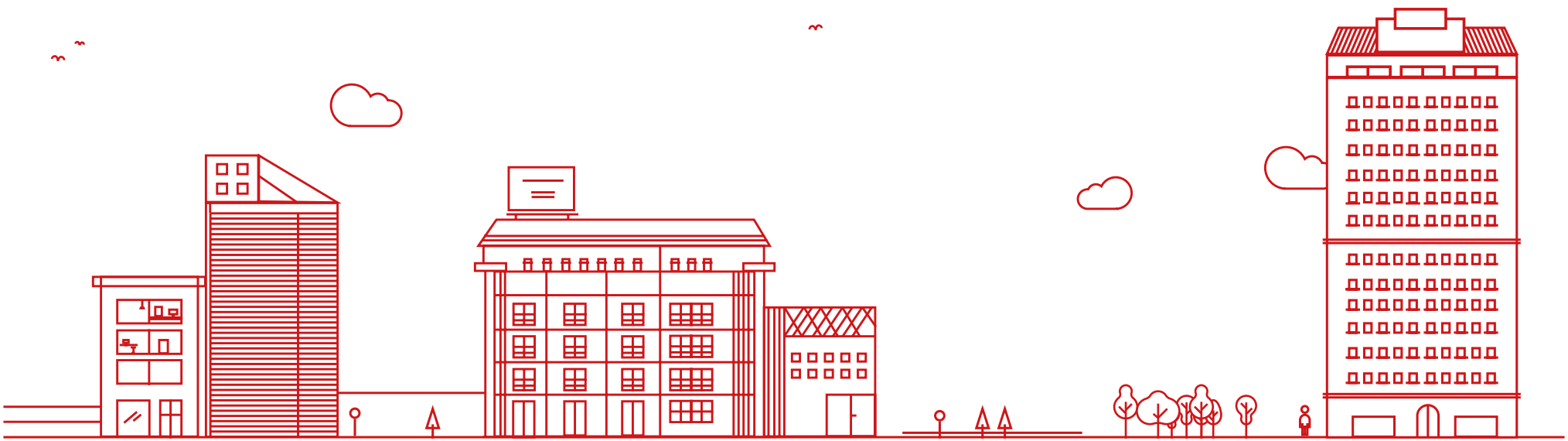
249 hôtels affectés

Rosen Hotels & Resorts

La chaine Rosen Hotels & Resorts est l'une des dernières victimes en date. Bien qu'elle n'ait pas communiqué d'information précise sur les conséquences de l'attaque**, l'infection de leurs terminaux de paiement par un malware a été confirmée pendant la période de septembre 2014 à février 2016.**

Inconnus de la chaine hôtelière, les pirates ont eu accès pendant 18 mois aux cartes de crédit utilisées par les clients des établissements Rosen alors que les terminaux de paiement étaient déja piratés.

Infecté sans le savoir pendant un an et demi



Ce n'est pas un phénomène passager

Le secteur hôtelier est devenu une cible de choix pour les gangs organisés de cyber-délinquants. Derrière chacune des attaques évoquées ci-dessus se trouve une forte motivation économique et la volonté farouche des pirates de rester anonyme.

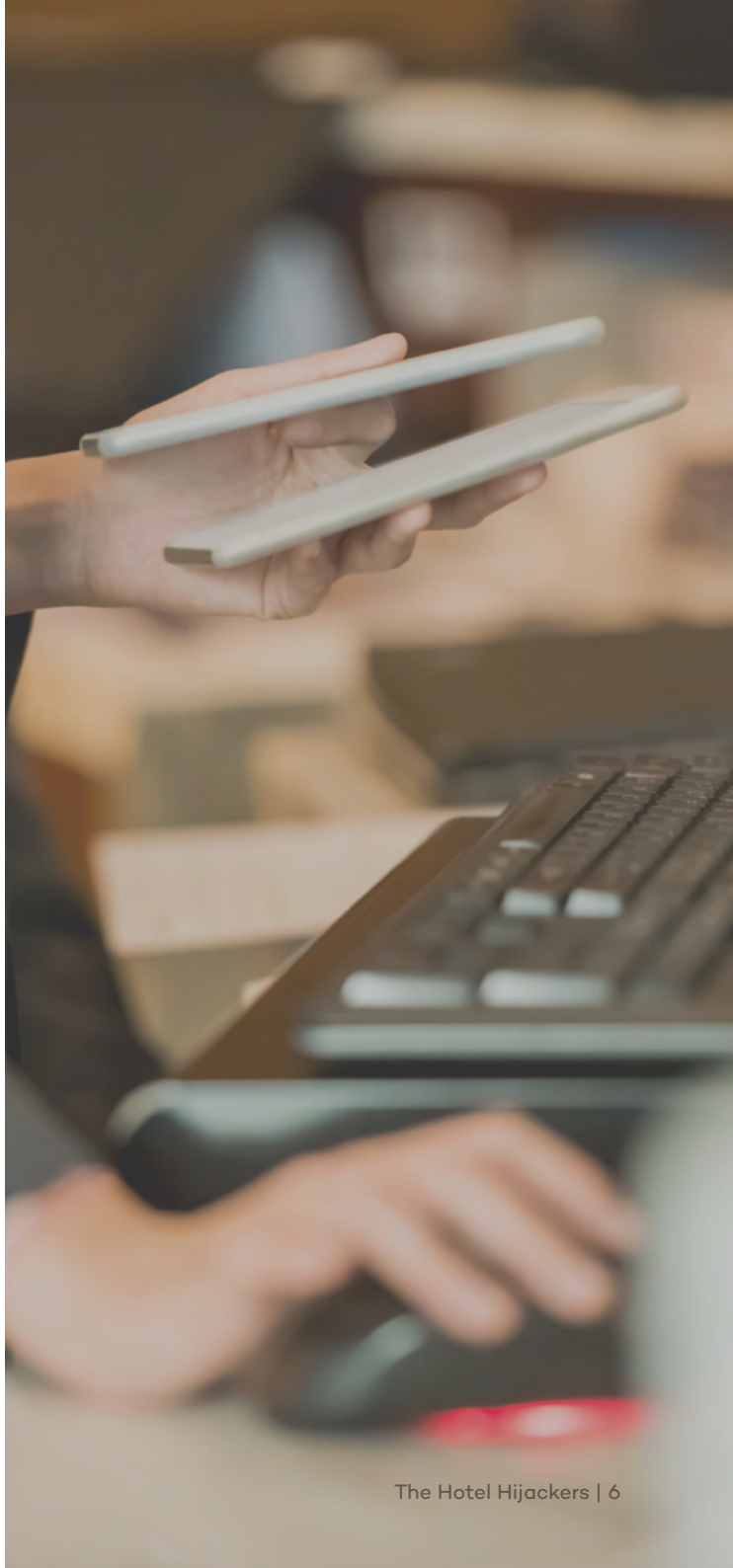
Le développement de malwares spécifiquement conçus pour dérober les données des cartes bancaires sur les systèmes de paiement des points de vente laisse supposer que ces pirates ne vont pas s'en aller de sitôt.

En plus d'affecter le secteur d'un point de vue économique, cette situation alarmante met aussi en danger la réputation des établissements, causant la panique et provoquant la défiance de leurs clients.

Nous devons rester vigilants

Pour prévenir ce type d'attaques ciblées, et leurs conséquences en termes de finance et de réputation, **les hôtels doivent renforcer la sécurité de leurs terminaux, systèmes et réseaux** et savoir choisir la solution la plus adaptée à leur problématique et à la spécificité de leur environnement métier.

Les protections système disponibles sur le marché n'offrent malheureusement pas un niveau de sécurité homogène ni en mesure de protéger toutes les types d'environnement numériques rencontrés.



La solution

Pour se protéger contre les menaces avancées et les attaques ciblées, il faut un système qui puisse garantir la confidentialité des données et le caractère privé des informations traitées.

Adaptive Defense 360 est **le premier et l'unique service de sécurité qui combine un antimalware parmi les plus performants du marché à un service EDR (Endpoint Detection & Response capable d'analyser et classifier tous les processus et programmes actifs sur votre réseau**.

Le fait de pouvoir surveiller en permanence 100% de ce qui est en cours d'exécution sur les terminaux et serveurs permet à Adaptive Defense 360 de détecter des malwares et des comportements anormaux que les autres outils de sécurité ne peuvent tout simplement pas voir. Cela permet également de pouvoir assurer une protection beaucoup plus efficace contre les malwares connus, les menaces Zero-Day, les attaques ciblées et les menaces persistantes avancées (APT). .

Avec Adaptive Defense 360, vous serez constamment au courant de ce qui se passe sur votre réseau, sur votre écosystème applicatif et au niveau de vos fichiers de données.

Des graphiques détaillés vous indiquent la chronologie des attaques détectées, les flux d'information, le comportement des processus en cours d'exécution, comment le malware s'est introduit dans le système, ses intentions, sa propagation, les informations ayant été compromises, etc..

En outre Adaptive Defense 360 vous aide à identifier et corriger facilement les vulnérabilités et les failles de sécurité tout en bloquant les applications indésirables (barres de navigation, PUP's et adwares, adds-on...)

Adaptive Defense 360: visibilité sans limite, contrôle absolu.

Retrouvez plus d'info sur :

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Visibilité sans limite, contrôle absolu

pandasecurity.com

panda

Plus d'information sur :

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

pour obtenir gratuitement votre version d'évaluation, appellez-nous

01 46 84 20 00

ou par email : **democloud@fr.pandasecurity.com**

panda