Hotel **Hijackers**

Großangelegter Datendiebstahl in der Hotelbranche

pandasecurity.com

panda

Hotel Hijackers

Nach all den Jahren, in denen wir im Bereich der IT-Sicherheit tätig sind, wissen wir eines sicher: Die Hauptmotivation für einen Cyberkriminellen ist Geld.

Ein unter Hackern derzeit besonders beliebtes Tool, um an vertrauliche Daten zu gelangen und daraus Profit zu schlagen, sind Trojaner: sich stets vervielfältigende, Informationen stehlende Malware-Samples, die unsere Computer und Geräte infizieren.

Prominentes Beispiel ist der Trojaner Cryptolocker. Diese Ransomware verschlüsselt wichtige Informationen auf den digitalen Geräten ihrer Opfer und zwingt den Nutzer, ein Lösegeld zu zahlen, um die Daten zurückzuerhalten.

Im Laufe der Zeit haben wir sowohl die „klassische“ Malware beobachtet, die mit einer einzigen Methode möglichst viele User treffen will, als auch die neuen Attacken, die individuell auf jedes Opfer zugeschnitten werden.

Eine Entwicklung ist dabei jedoch besonders bemerkenswert: In neuester Zeit haben es die Cyberkriminellen vermehrt auf Hotelketten abgesehen.

Warum Hotels?

Hacker betrachten Hotels als besonders lukratives Geschäft.

Der Grund dafür liegt auf der Hand: Von der Buchung eines Zimmers bis hin zu Zahlungen, die in den Geschäften und Restaurants des Hotels getätigt werden – Hotelketten verfügen über riesige Mengen an vertraulichen und privaten Daten, die sie in komplexen digitalen Netzwerken speichern. Denn in kaum einem anderen Wirtschaftsbereich gibt es eine so große Menge an wechselnden und ständig neu hinzukommenden Kunden, die gleich bei der ersten Buchung ihren Namen, Adresse, Zahlungsdetails etc. preisgeben.

Wenn Sie also kürzlich in einem Hotel übernachtet haben, sollten Sie vielleicht Ihre Kreditkartenabrechnung noch einmal überprüfen...

Die Fakten sprechen für sich

In puncto Hackerangriffe hat das Jahr 2015 im Hotelgewerbe einen neuen Meilenstein gesetzt.

Nie zuvor wurden so viele Hotels, unabhängig von ihrer Größe, Opfer von Cyberverbrechen wie im vergangenen Jahr.

Dabei haben Hacker ihr Augenmerk nicht nur auf Hotels gerichtet, sondern auch auf deren Dienstleister.

White Lodging

White Lodging verwaltet eine Reihe namhafter Hotels wie Hilton, Marriott, Hyatt, Sheraton und Westin Hotels. Das in den USA ansässige Unternehmen war bereits im Jahr 2013 Opfer einer großen Cyberattacke, bei der Kredit- und Kundenkarteninformationen von 14 seiner Hotels gestohlen wurden.

2015 wurde White Lodging Opfer eines weiteren Hackerangriffs. Diesmal waren zehn Hotels betroffen, von denen einige bereits Opfer der vorhergehenden Attacke waren. Bei diesem zweiten Angriff stahlen die Hacker noch umfangreicheres Datenmaterial: Kreditkartendaten, Kundennamen, Kundennummern, Sicherheitscodes und Ablaufdaten.

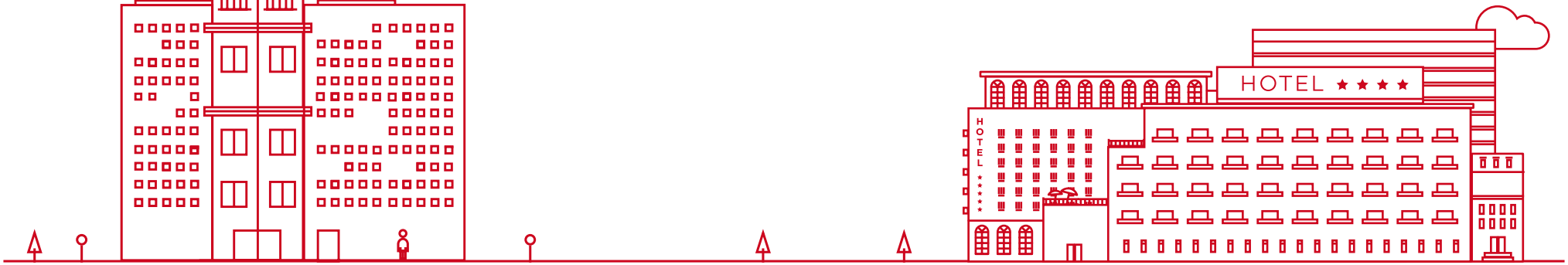
24 Hotels betroffen

Mandarin Oriental

Das luxuriöse Mandarin Oriental wurde im März 2015 angegriffen. Malware infizierte Point-of-Sale (POS) - Terminals in einigen europäischen und amerikanischen Hotels dieser Gruppe.

Die Malware war eigens für diese Art von Zahlungssystemen entwickelt, um gezielt Kreditkarteninformationen zu stehlen.

Tausende von Kreditkarten gefährdet



Trump Hotels

Zwischen Mai 2014 und Juni 2015 wurden sieben ihrer Hotelbetriebe angegriffen.

Wie das Unternehmen bestätigte, wurden Kreditkartendaten der Kunden über infizierte POS-Terminals und Computer in ihren Restaurants, Geschenkeläden und anderen Geschäften gestohlen.

Ein einziges Jahr reichte den Cyberkriminellen aus, um Unmengen vertraulicher Informationen zu erhalten.

Dutzende infizierter Computer und POS-Terminals

Hard Rock Las Vegas

Ein Angriff infizierte POS-Terminals in den Restaurants, Bars und Geschäften des Hard Rock Las Vegas. Es waren jedoch keine Geräte im Hotel oder Casino betroffen.

Über einen Zeitraum von sieben Monaten, von September 2014 bis April 2015, erlebte das Hard Rock Las Vegas Hackerangriffe, bei denen Daten von insgesamt 173.000 Karten aus seinen Restaurants, Bars und Geschäften gestohlen wurden.

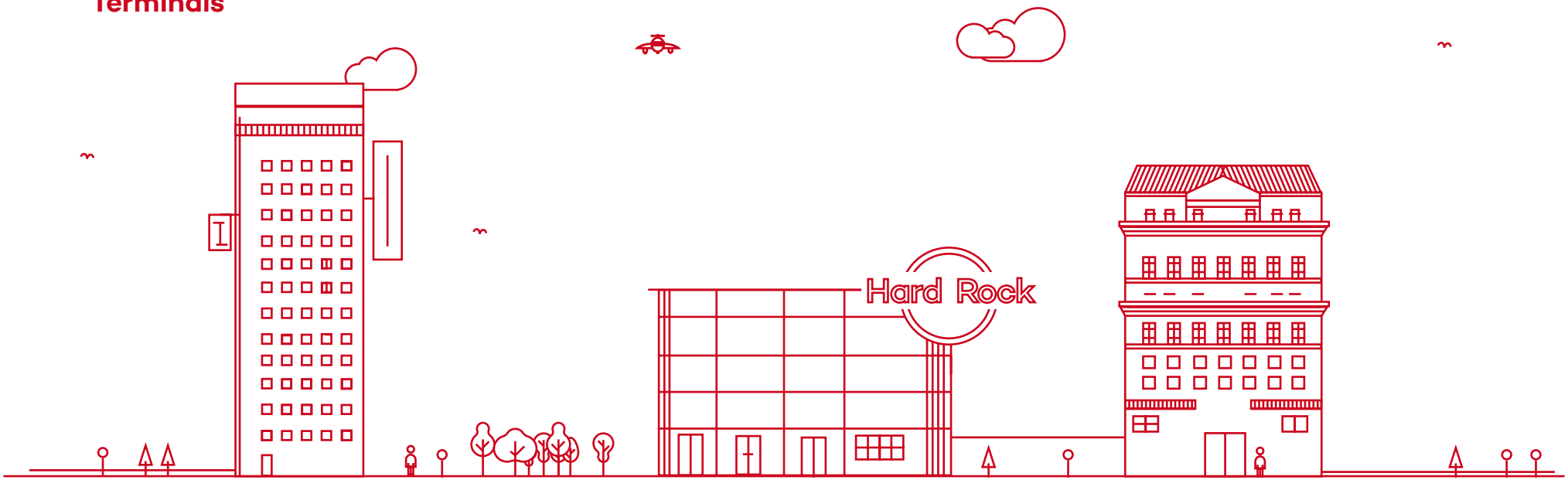
Daten von 173.000 Kreditkarten gestohlen

Hilton Worldwide

Im November 2015 veröffentlichte das Unternehmen Hilton Worldwide eine Pressemitteilung, in der es bestätigte, Opfer einer Cyberattacke geworden zu sein.

Genaue Angaben über die Art und Weise des Hackerangriffs machte das Unternehmen nicht. Es wurde jedoch bekannt, dass Kreditkarteninformationen der Hilton-Kunden gestohlen wurden. Persönliche PIN-Codes blieben von dem Diebstahl dem Vernehmen nach unberührt.

Zugriff auf vertrauliche Daten



Starwood Hotels & Resorts

Ungefähr zur selben Zeit, zu der sich der zuvor erwähnte Angriff auf die Hilton Hotels ereignete, gab Starwood bekannt, dass sie Opfer eines ähnlichen Cyberangriffes geworden seien.

105 Hotels der Starwood-Kette wurden angegriffen (darunter Sheraton, St. Regis, Westin). Bis dato war dies der größte Cyberangriff dieser Art in der Hotelbranche.

Starwood veröffentlichte eine Liste mit den Hotels, in denen Malware ihre POS-Terminals infiziert hatte.

105 Hotels betroffen

Hyatt

Der Rekord von Starwood war nur von kurzer Dauer, denn nur wenige Tage später wurde bekannt, was als die bisher größte Cyberattacke in der Hotelgeschichte gilt:

Wie die Hotelkette Hyatt im Dezember 2015 bestätigte, kam es zwischen August und Dezember 2015 zu Malware-Infektionen von POS-Terminals der Hyatt-Kette, bei denen diverse Kreditkarteninformationen ihrer Kunden gestohlen wurden.

Betroffen waren 250 Hyatt-Hotels weltweit, darunter auch die deutschen Hyatt-Betriebe in Berlin, Köln, Düsseldorf, Hamburg und Mainz.

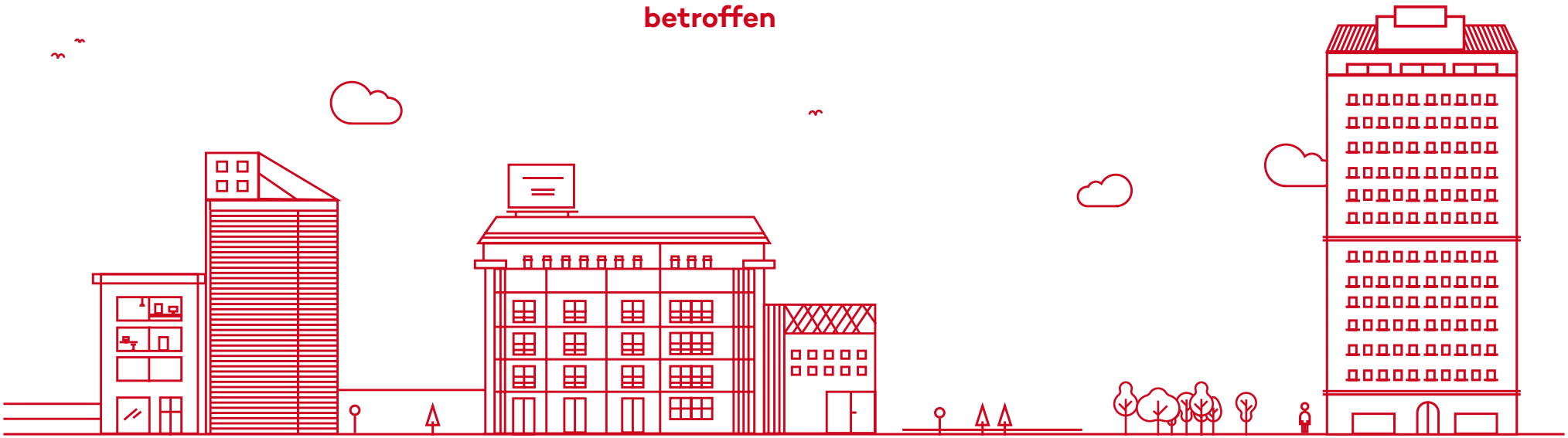
250 Hotels betroffen

Rosen Hotels & Resorts

Das jüngste Opfer sind die Rosen Hotels & Resorts. Am 4. März 2016 bestätigte das Unternehmen, dass seine POS-Terminals von September 2014 bis Februar 2016 mit Malware infiziert wurden.

Während dieses Zeitraumes griffen die Cyberkriminellen unbemerkt auf die Kreditkartendaten der Rosen-Kunden zu. Dabei stahl die Malware die Namen der Karteninhaber, die Kartennummern, Ablaufdaten und Kartenprüfnummern.

1,5 Jahre infiziert, ohne es zu merken



Hotel Hijacking ist keine Eintagsfliege

Es gibt ein echtes wirtschaftliches Interesse hinter diesen großangelegten Hackerangriffen und die Neugier, wie lange die jeweilige Attacke unentdeckt bleiben kann. Die Hotelbranche ist zu einem der Hauptziele für Cyberkriminelle geworden.

Inzwischen gibt es Malware, die eigens dafür entwickelt wird, wichtige Kreditkarteninformationen von POS-Systemen abzugreifen. Das lässt darauf schließen, dass diese Art von Hackerangriffen nicht so bald verschwinden wird.

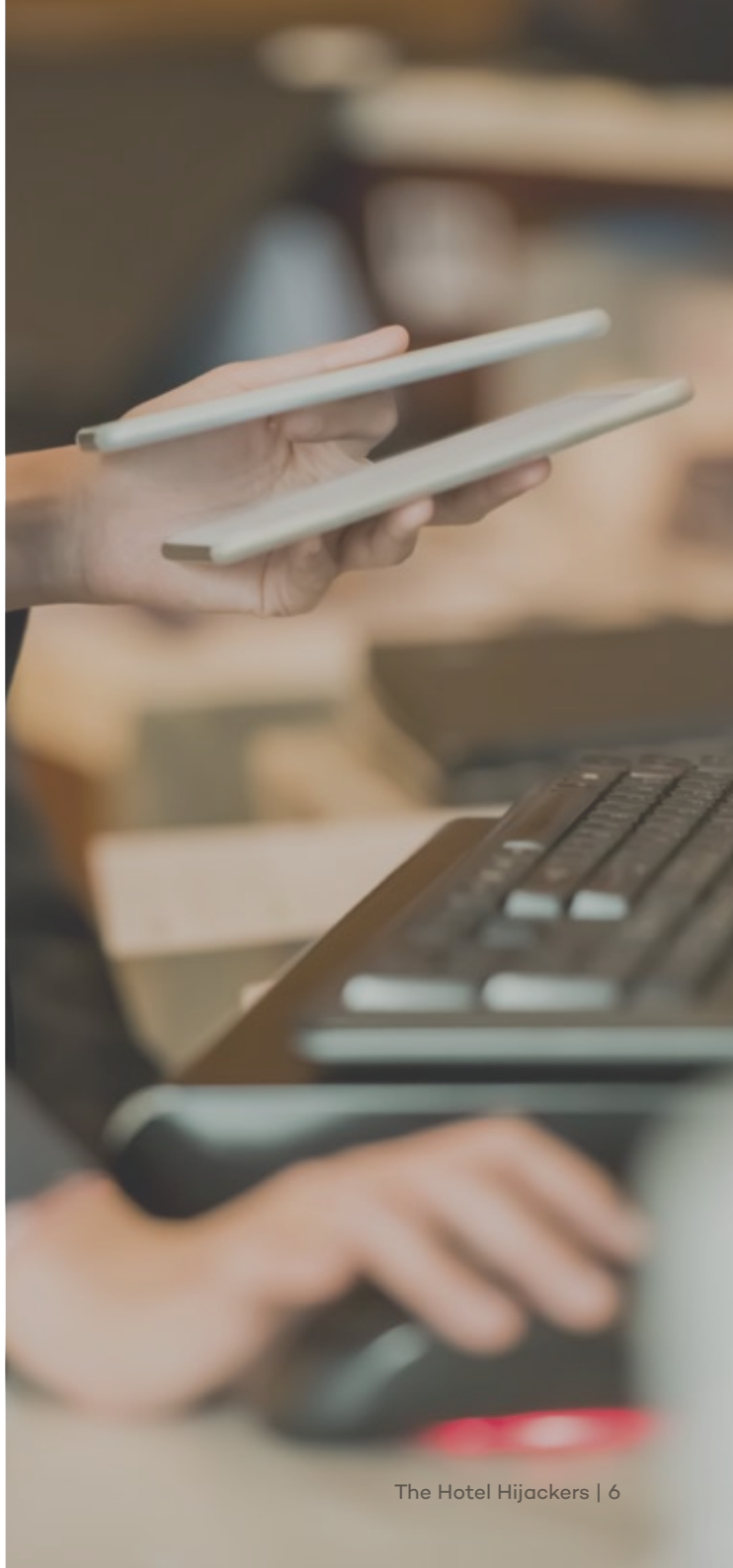
Diese alarmierende Situation trifft die Hotelbranche nicht nur wirtschaftlich, sondern gefährdet zudem ihren Ruf, verursacht Misstrauen bei den Kunden und destabilisiert das Geschäft.

Die Branche muss sich schützen

Malware, die POS-Terminals infiziert, um Kreditkartendaten zu stehlen, und gezielte Hackerattacken gegen Hotelsysteme, um vertrauliche Informationen zu entwenden - das sind nur zwei Beispiele dafür, wie Cyberangriffe ablaufen können und welche Folgen diese nach sich ziehen.

Hotels müssen daher unbedingt die Sicherheit ihrer Netzwerke, Geräte und Systeme verstärken und wissen, wie sie das richtige Schutzsystem für ihr Unternehmen auswählen.

Denn nicht jedes Schutzsystem wird für diese Branche funktionieren, weil nicht alle dasselbe Sicherheitslevel bieten und in der jeweiligen Geschäftsumgebung den passenden IT-Schutz liefern.



Panda bietet die passende Lösung

Um uns vor fortschrittlichen Bedrohungen und gezielten Angriffen zu schützen, benötigen wir ein System, das die Vertraulichkeit von Daten, den Schutz von sensiblen (Kunden-) Informationen und einzigartigem Firmenwissen gewährleistet.

Adaptive Defense 360 ist ein neu entwickeltes IT-Schutzsystem auf höchstem technischem Niveau, das erstmals Endpoint Protection (EPP) und Endpoint Detection and Response (EDR)-Fähigkeiten kombiniert.

Adaptive Defense 360 kann Malware und ungewöhnliches Verhalten erkennen, weil es alle laufenden und ausgeführten Prozesse klassifiziert. Dies können blacklist-basierte Anti-Malware-Systeme nicht.

Deshalb schützt es sowohl vor bekannter Malware als auch vor unbekannter Malware, wie Zero-Day-Bedrohungen, APTs (Advanced Persistent Threats) und direkten Angriffen.

Mit Adaptive Defense 360 wissen Sie immer, was mit jeder Ihrer Dateien und Prozesse geschieht.

Detaillierte Diagramme aller ausgeführten Aktionen geben einen klaren Überblick über alle Ereignisse, die im Netzwerk passieren. Zeitleisten und Heatmaps geben visuelle Informationen über die Herkunft der Malware-Verbindungen, wie diese ins System gelangt sind, welche Dateien sie erstellt haben oder erstellen wollten und vieles mehr.

Mit Adaptive Defense 360 lassen sich Schwachstellen leicht erkennen und beseitigen. Gleichzeitig verhindert es die Ausführung unerwünschter Prozesse (wie die Installation zusätzlicher Navigationsleisten, Adware, Add-ons usw.).

Weite Informationen unter: http://www.pandasecurity.com/germany/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Uneingeschränkte Transparenz, absolute Kontrolle

pandasecurity.com

panda

Weitere Informationen unter:

pandasecurity.com/germany/business/adaptive-defense/

Rufen Sie uns an:

02065 961-200

Kontaktieren Sie uns per E-Mail:

vertrieb@de.pandasecurity.com

panda