The Hotel **Hijackers**

pandasecurity.com

panda

The Hotel Hijackers

After all these years we've been in the computer security business, there is one thing we know for sure: a cyber-criminal's main motivation is always money.

That's why the hackers use Trojans to get the confidential data: the always-multiplying, information-stealing bugs that infect our computers and devices.

One example of this is **CryptoLocker, a popular attack that uses ransomware to encrypt important information** then forces the victim to pay a ransom to get it back.

Over time, we've witnessed both the "classic" malware and the new attacks that are devised specifically for each victim, and how companies are dealing with these attacks.

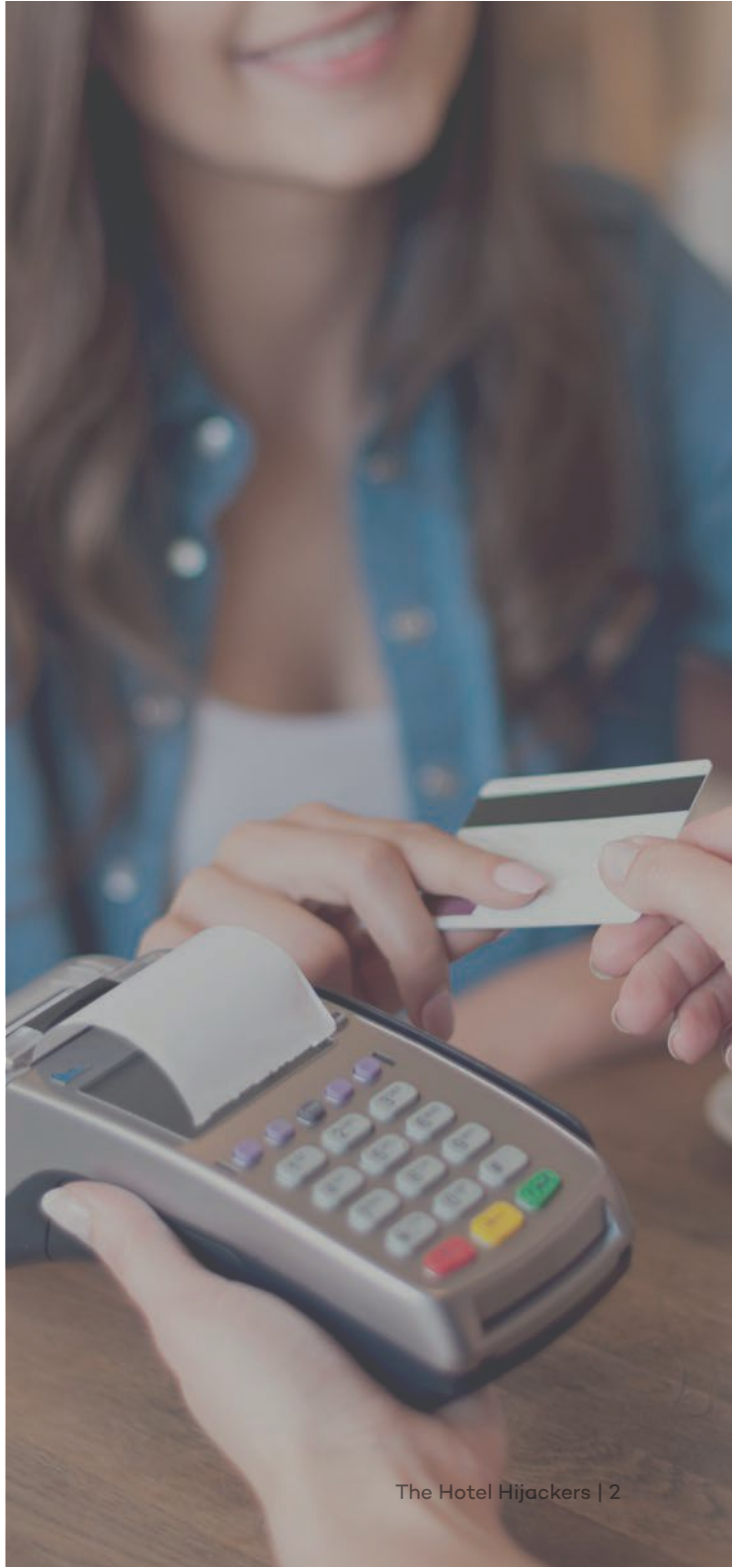
Most recently, these cyber-criminals have been going after hotel chains.

Why hotels?

Hackers see hotels as juicy business.

When a phisher considers a hotel, they are thinking of how they can "fish" from the millions of rooms, used by millions of customers, which generates millions of dollars.

From booking a room to the payments made at shops and restaurants, hotel chains have complex networks that save enormous amounts of sensitive and private data, just waiting to be compromised. If you stayed at a hotel recently, you might want to double-check your credit card statements...



A promised history

2015 set a new milestone in this sector.

By 2015, **most of the hotels, regardless of size, have been victims of cyber-crimes**.

Cyber-criminals also have their eyes set on companies that provide services for the hotels.

White Lodging

White Lodging manages a number of well-known hotels like the Hilton, Marriott, Hyatt, Sheraton, and Westin hotels. Although they are more of a hotel management company than a hotel chain, they were still victims of a big cyber-attack that was made public in 2014. In 2013, **customer credit card and debit card information was compromised from fourteen of their hotels**.

Two years later, they suffered another attack, this time hitting ten hotels (some of them were also victims of the previous attack). The hackers came back for more: stealing data from credit cards like customer names, numbers, security codes, and expiration dates. According to White Lodging, this attack was different from the first one in 2013.

24 hotels affected

Mandarin Oriental

The luxurious Mandarin Oriental was attacked in March 2015. **Malware infected POS** (Point-of-Sale) terminals from some of the group's hotels in Europe and America.

The malware was specially designed and directed towards these type of machine systems, allowing them to steal credit card information.

Thousands of credit cards compromised

Trump Hotels

They were attacked in seven of their establishments from May 2014 to June 2015.

As they acknowledged, **customer credit card data was stolen from infected POS terminals and computers** at their restaurants, gift shops and other businesses.

Just one year was enough for the criminals to get tons of confidential information.

Dozens of infected computers and POS terminals

Hard Rock Las Vegas

An attack infected some of the POS terminals from their restaurants, bars and shops. But it didn't affect any devices in the hotel or casino.

Over the span of seven months, from September 2014 to April 2015, the Hard Rock Las Vegas faced **attacks leading to a total of 173,000 stolen cards** from their restaurants, bars and shops.

But they weren't the only hotel/casino affected. FireKeepers Casino Hotel, in Battle Creek, was another victim of 2015.

173,000 stolen cards

Hilton Worldwide

In November 2015, Hilton Worldwide issued a press release acknowledging that they were victims of a cyber-attack.

They didn't give very much information about what happened but it is known that **customers' complete credit card information was compromised**.

Fortunately, PIN and other personal information codes were untouched.

Access to confidential information

Starwood

Around the same time as the previous Hilton attack, Starwood announced they were victims of a similar cyber-attack.

105 hotels in the Starwood chain were attacked (Sheraton, St. Regis, Westin, W, etc.), making it **the biggest attack of this kind in the hotel sector at that very moment**.

They published a list naming the hotels where the malware infected their POS terminals.

105 hotels affected

Hyatt

The Starwood's record was quite short-lived. Then came what we now know as the biggest cyber-attack in hotel history.

The Hyatt hotel chain confirmed that a press release resulted in **infected point-of-sale terminals from 249 hotels of their hotels in 54 countries**.

From July to September 2015, their POS terminals -once again- were infected and all customer credit card information was stolen.

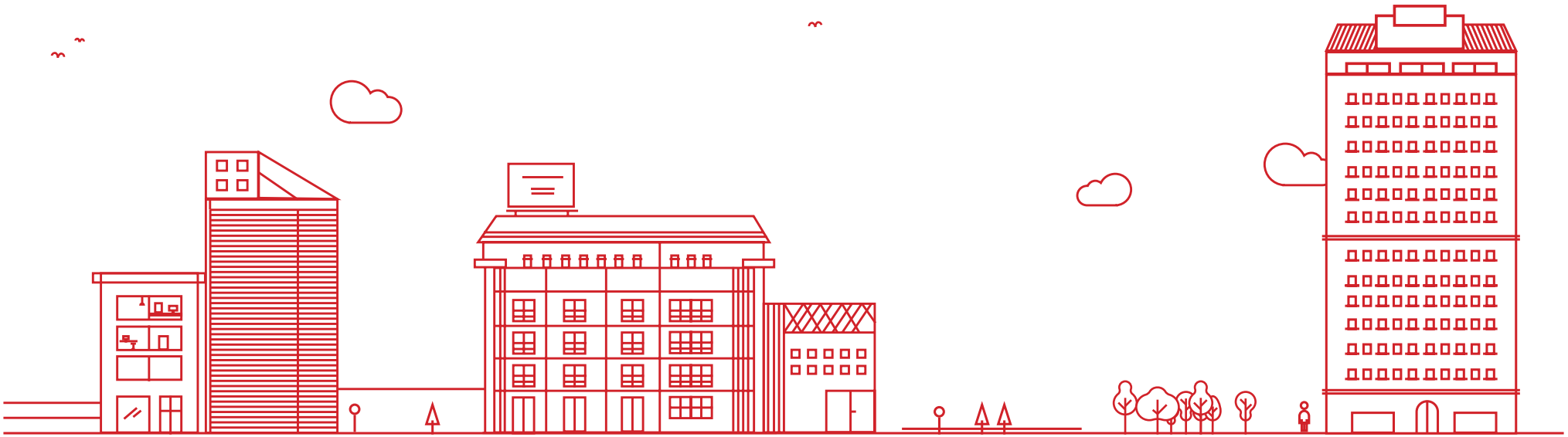
249 hotels affected

Rosen Hotels & Resorts

The most recent victims are the Rosen Hotels & Resorts. While they have not given exact information about the theft, they have confirmed that their **point-of-sale terminals were infected with malware from September 2014 until February 2016**.

Unknown to the hotel chain, the thieves accessed customer credit cards that were used in the Rosen establishments throughout the last year and a half, while their POS systems were infected.

1.5 years infected without realizing it



This is not a fad

There is real economic interest behind these attacks and curiosity about remaining unknown. **The hotel sector has become one of the main targets for cyber-criminal gangs**.

Along with motivation, there is malware that is designed specifically to scrape important credit card information from the POS systems, making it clear that these hackers won't be going away anytime soon.

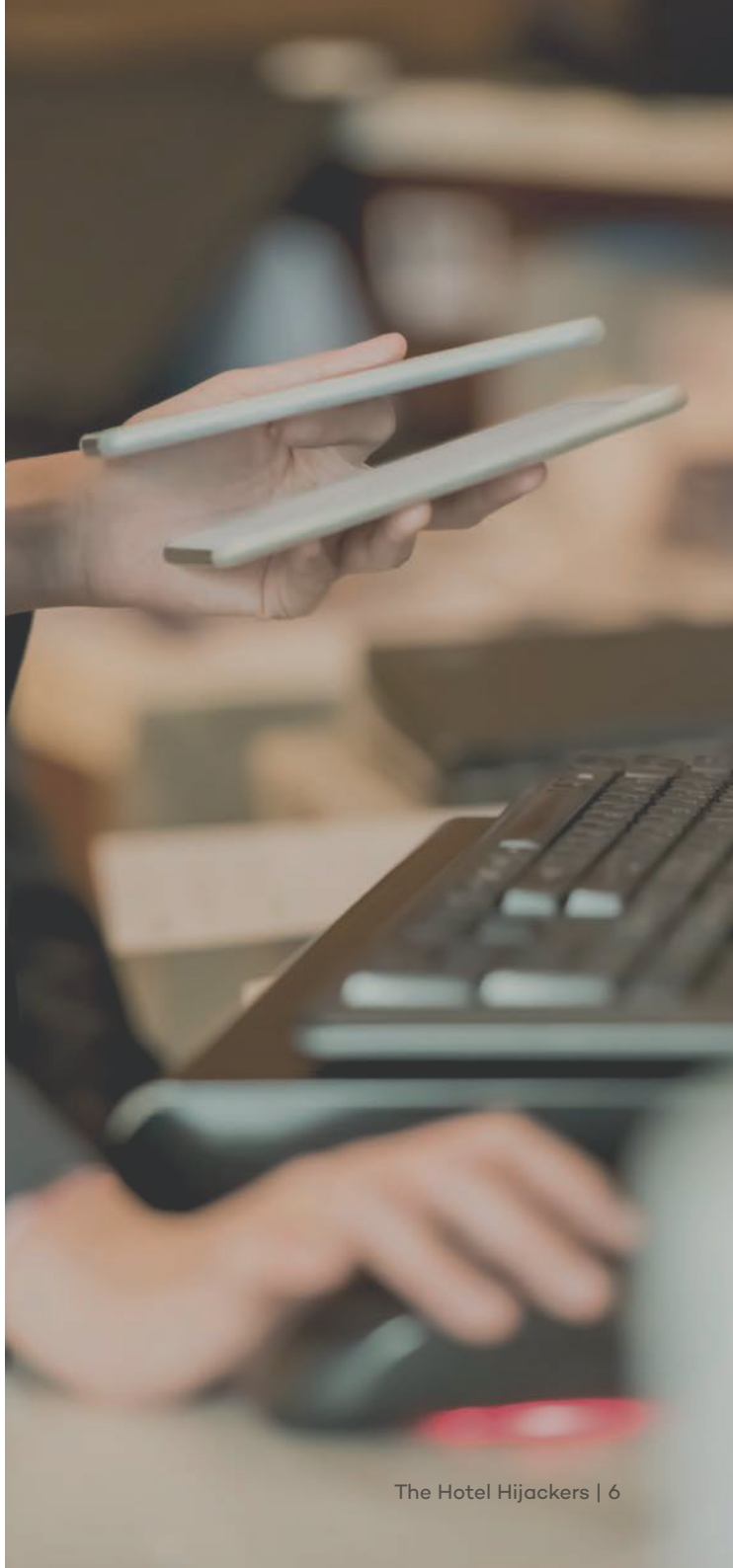
This alarming situation not only affects the sector economically, but it endangers their reputation, causes panic among their customers and destabilizes the business.

We must be alert

Malware that infects point-of-sale terminals to steal credit card data, and targeted attacks against hotel systems to steal confidential data, are two examples of what can happen during a cyber-attack. These kind of attacks have severe repercussions to a hotel's finances and reputation.

Hotels need to reinforce security on their network, devices and systems, and know how to choose the right protection system for their business.

Not any protection system will work for this sector, because not all of them offer the same level of security, and not all of them can protect in any digital ecosystem or business environment.



The solution

To protect against advanced threats and targeted attacks we need to have a system that guarantees Data Confidentiality, Privacy of Information and Business Reputation, and Legacy.

Adaptive Defense 360 **is the first and only cyber security service that combines the most effective traditional antivirus and the latest advanced protection with the capability of classifying all executed processes**.

Adaptive Defensive 360 can detect malware and strange behaviors that other protection services cannot because it classifies all running and executed processes.

Thanks to that, it can ensure protection against known malware and advanced Zero-Day Threats, Advanced Persistent Threats and Direct Attacks.

With Adaptive Defense 360, you will always know what happens to each of your files and processes.

Detailed graphs show everything that takes place on the network: timeline of threats, flow of information, how the active processes behave, how the malware entered the system, where it is going, who intended to do what and how they got that information, etc.

Adaptive Defense 360 makes it easy to discover and fix those vulnerabilities while also preventing the unwanted (like navigation bars, adware, add-ons...).

Adaptive Defense 360: limitless visibility, absolute control.

More info at:

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

More information at:

1-407-215-3020

sales@us.pandasecurity.com

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda