Ransomware Hijacks Hotel Smart Keys to Lock Guests Out of their Rooms

---

Posted by Hermes 02/19/2017

What's the worst that could happen when a Ransomware hits a Hotel?

Recently, hundreds of guests of a luxurious hotel in Austria were locked in or out of their rooms when ransomware hit the hotel's IT system, and the hotel had no choice left except paying the attackers.

Today, we are living in a digital age that is creating a digital headache for people and organizations around the world with cyber attacks and data breaches on the rise.

Ransomware is one of them.

The threat has been around for a few years, but during 2016, it has turned into a noxious game of Hackers to get paid effortlessly by targeting hospitals, Universities, private businesses and even police departments and making hundreds of millions of dollars.

Now, the **Romantik Seehotel Jäegerwirt 4-Star Superior Hotel** has admitted it paid €1,500 (£1,275/$1,600) in Bitcoin ransom to cybercriminals who managed to break into their network and hack their electronic key card system that prevented its guests from entering or leaving their rooms.

The luxury hotel with a beautiful lakeside setting on the Alpine Turracher Hoehe Pass in Austria, like several other hotels in the industry, has a modern IT system that includes key cards for its hotel doors, which could not be programmed.

Also Read: This Tool Detects Never-Seen-Before Ransomware Before It Encrypts Your Data

According to the hotel management, the hotel has been hit multiple times by hackers, but this time they managed to take down the entire key system, preventing its guests to getting in or going out of their rooms, reported The Local.

Besides gaining control of the electronic key system, the hackers even gained control over the general computer system, shutting down all hotel computers, including the reservation system and the cash desk system.

Once the hotel made the payment, the system was completely restored that allowed the hotel staff to gain access to the network and hotel guests to enter and exit their rooms.

What's interesting? Even after the hotel fulfilled the hackers demand, the hackers left a backdoor to the hotel system in an attempt to conduct another cyber attack later.

Fortunately, the security standards of the hotel had been improved by its IT department, and critical networks had been separated to thwart the attack, giving attackers no chance to harm the hotel again.

Furious hotel managers decided to go public with the incident to warn others about the dangers of cyber attack, with Managing Director Christoph Brandstaetter said:

"The house was totally booked with 180 guests; we had no other choice. Neither police nor insurance helps you in this case.

The restoration of our system after the first attack in summer has cost us several thousand Euros. We did not get any money from the insurance so far because none of those to blame could be found.

Every euro that is paid to blackmailers hurts us. We know that other colleagues have been attacked, who have done similarly."

The Ransomware had stolen the nights of many businesses and organizations, as they would often be blamed to fight up to this nasty threat.

Ransomware criminals often demand the ransom in Bitcoin (BTC) for the surety of not getting caught, as Bitcoin transactions are non-trackable due to its decentralized nature.

The frequent payment to Ransomware encourages criminals to stash the cash and develop a more enticing framework for the next target. So, instead of paying or encouraging this scheme, keep your software and systems updated and avoid clicking suspicious links. -Courtesy of SynEVOL
