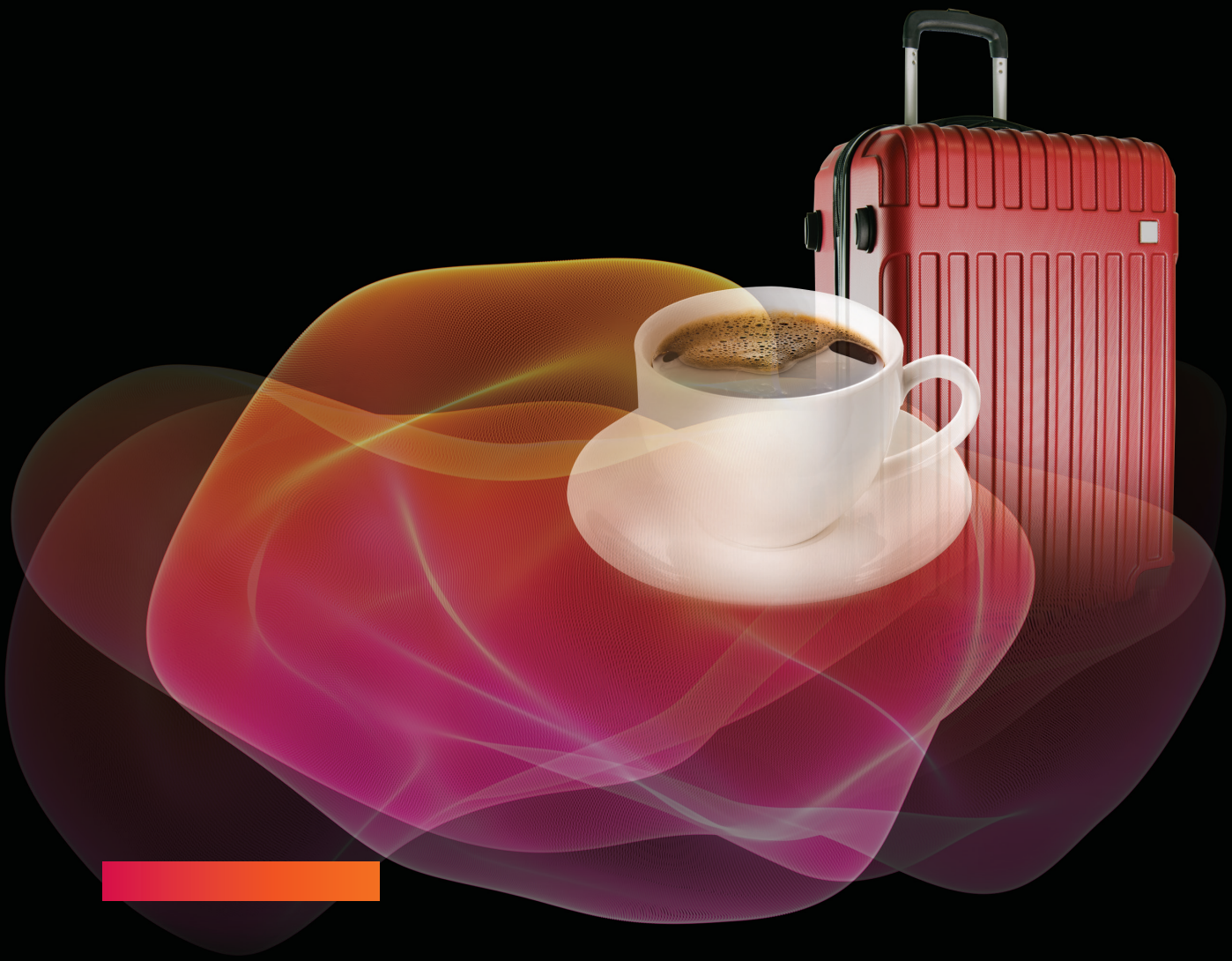
MORPHISEC
Moving Target Defense



MORPHISEC

2019 HOSPITALITY GUEST CYBERSECURITY THREAT INDEX

The $124 million fine recently imposed by UK regulators against Marriott for the Starwood hotel breach was the hospitality industry's latest indication that subpar cyber defenses can have bottom-line business ramifications. In fact, the penalty is only a fraction of the billions of dollars that Marriot is projected to lose on that breach, which exposed the personal information of 339 million guests and is one of the five most significant breaches in history.

Alongside the threat of fines, IT costs and legal fees, hospitality companies of all kinds are also battling a perception problem in the minds of guests when it comes to cyber safety. The Starwood breach drove home the serious imbalance that exists, with hackers infiltrating a trusted hotel chain's database and operating undetected for more than four years.

These sophisticated attacks on the hospitality industry are only becoming more frequent and advanced. In addition to Marriott, nearly every major hotelier — Hilton Worldwide Holdings, InterContinental Hotels, Radisson, Trump Hotels, Loews Hotels, and Hyatt Hotels, among others — has dealt with some type of breach over the past few years. Just as cybercriminals target banks and financial institutions, they are drawn to the hospitality industry for the payment information they hold on millions of customers. And with their widespread networks and multiple entry points for attack, hospitality establishments make a significantly easier mark.

With each new attack targeting the hospitality sector, cybercrime groups also display signs of tactical evolution and new evasive abilities. For instance, in June of this year, Morphisec found that FIN8, a cybercrime group most known for targeting the retail industry, was actively targeting Point-of-Sale (POS) systems within hospitality companies in the U.S. and abroad.

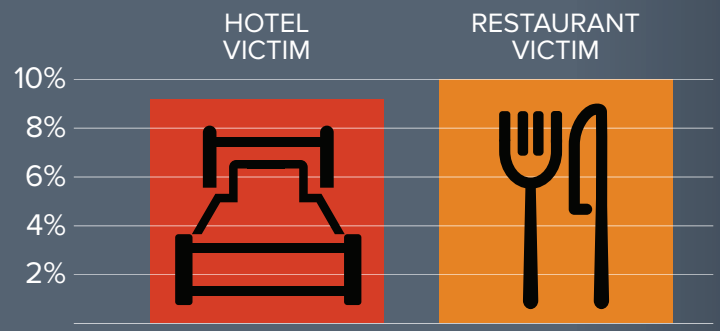
Hotels are not the only hospitality targets for POS attacks; restaurants are also highly vulnerable. According to the 2018 Trustwave Global Security Report, 60% of successful cyberattacks on food and beverage establishments are made through POS intrusions. In addition, major cybercrime groups such as FIN7 have breached restaurant systems via phishing emails that contain weaponized Microsoft Office attachments.

As Morphisec continues to assist hospitality providers with improving defenses and protecting customer financial data and personal information, we decided to examine how the threat of cyberattacks is impacting the mindset of consumers as they do business with hotels, restaurants and various types of entertainment companies.

To take the pulse of consumers in the U.S., we commissioned Morphisec's 2019 Hospitality Guest Cybersecurity Threat Index, a survey administered in Q3 to 1,000 U.S. consumers aged 18+ and weighted by age, region, and gender. Here's what we found:

9% of Consumers Say They've Been the Victim of a Hotel Data Breach or Cyberattack; 10% a Victim of a Restaurant Breach

Q: Have you been the victim of a hotel or restaurant data breach?



Considering the ramp-up in attacks, it's no surprise that a sizable portion of the population has been directly affected. One-in-ten U.S. consumers over 18 years old say they have been the victim of a data breach or cyberattack through visiting a restaurant. This was slightly more than the 9% who say they have been a cybercrime victim through booking and staying at hotels.

With the estimated 2019 U.S. population of those over 18 hovering around 255 million, we can extrapolate that more than 22 million U.S. customers have been the victim of a cyberattack through their business with hotels. And this figure is limited to customers aware that their data has been compromised – despite mandatory alerts, many never discover that they were a breach victim. It should also be pointed out that while this number may seem small given the 300 million-plus customers affected by the Starwood breach, U.S. guests were only a fraction of the global total in that attack.

Meanwhile, more than 25 million consumers in the U.S. are aware that their restaurant visits cost them their data along with their meal. With major restaurant chains such as Applebees, Darden Restaurants, Dunkin' and Panera all experiencing cyberattacks in the past two years alone, it's likely that the actual number of consumers impacted is much higher.

Nearly 70% of Guests Don't Believe the Hotels They Stay at Are Investing Enough in Cybersecurity

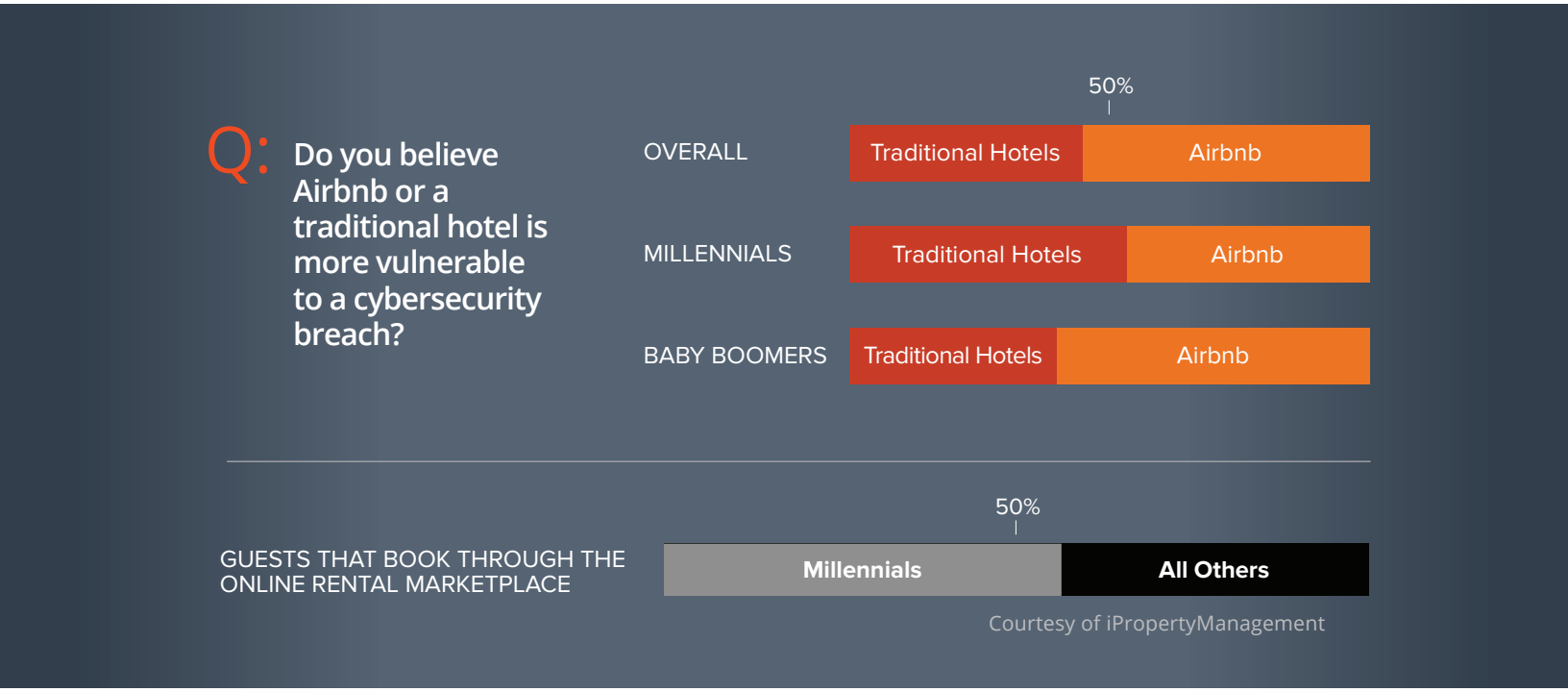
Q: Do you believe the hotels you frequent are investing enough in cybersecurity to protect your personal and payment information?

With tens of millions of guests aware that their hotel stay led to the compromise of their data, it's understandable that the vast majority would like the hotels they frequent to invest more in their cyber defenses.

Over 69% of guests said that they believe their chosen accommodation provider is not investing enough to protect their personal and payment information. This despite the fact that the 2019 Lodging Technology study found hospitality IT leaders rate improving data and payment security as a top strategic goal when it comes to their technology spend. It also found that the industry has made significant strides, with the number of hotels with breach protection doubling since 2017.

The U.S Department of Commerce, however, shares the sentiments of consumers. Following the Marriott breach, U.S. Commerce Secretary Wilbur Ross noted that ***"many companies have been scrimping on the cybersecurity budget"*** — both in the hospitality sector and beyond.

Millennials Believe They Are More Vulnerable to a Cybersecurity Breach When Booking with a Traditional Hotel vs. Airbnb



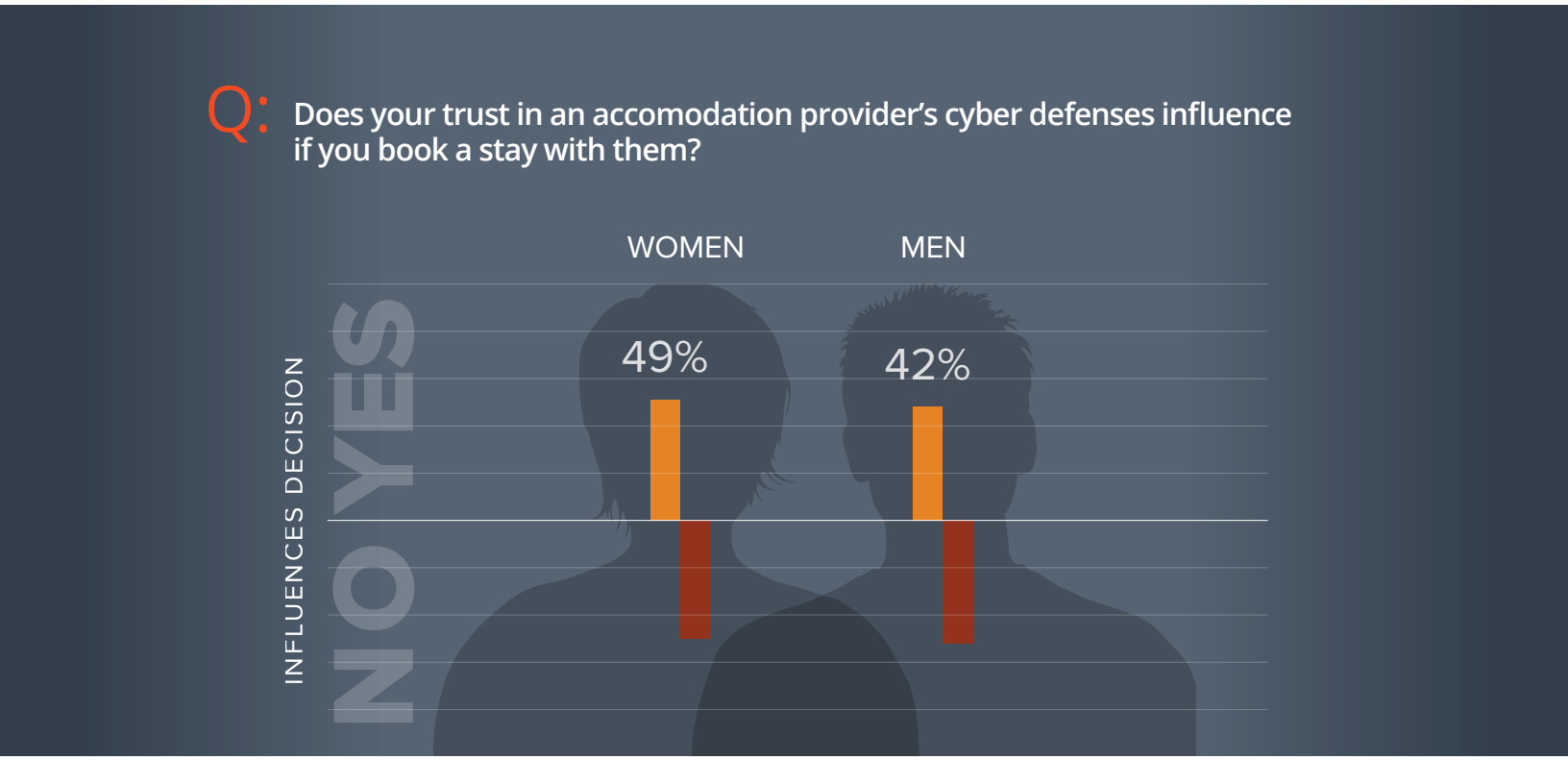
Given that Airbnb now takes around 10% of all U.S. lodging, we also wanted to look at guest perception on the cyber defenses of traditional hotels versus an online rental marketplace.

Overall, guests that thought Airbnb (54%) was more vulnerable to cyber attacks nudged out those that felt traditional hotels were more vulnerable (46%). However, the numbers tell a different story when broken down by demographic.

Millennials (25- to 34-year-olds), actually thought that traditional hotels (53%), not Airbnb (47%), were more vulnerable to cyberattacks. Not surprisingly, millennials are also Airbnb's largest guest demographic, making up 60% of all guests that book through the online rental marketplace according to iPropertyManagement. Given that the company put into place mandatory multi-factor authentication and other online security measures, and recently appointed a Chief Trust Officer, they may have a valid point.

Meanwhile, Baby Boomers, or those 65+, were adamant that Airbnb (60%) was more vulnerable to a cyberattack versus traditional hotels (40%). This likely stems from unfamiliarity with Airbnb — according to AARP only 10% of Baby Boomer travel accommodations utilized online home rental sites such as Airbnb or VRBO — or perhaps a lack of awareness of how accommodation providers are most vulnerable to cyberattacks.

Nearly Half of Guests Say Their Trust in a Hotel's Cyber Defenses Influence if They Book a Stay with Them



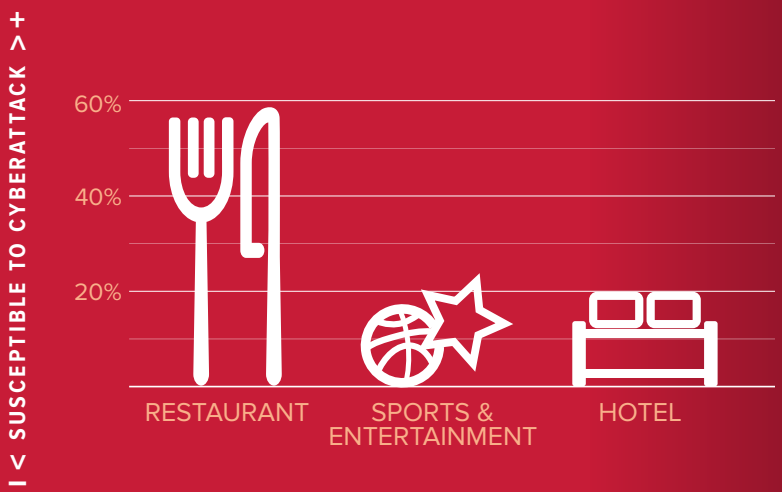
With an overwhelming number of consumers stating that the hotels they frequent don't spend enough to protect their information, we also examined how lack of trust in a hotelier's cyber defense could impact current and future business.

In fact, nearly half (46%) of respondents say their trust in a hotel's cyber defenses does influence if they book a stay with them. That number was even higher for female guests, with 49% noting a lack of trust in cyber defenses impacting bookings vs. 42% of their male counterparts.

Trust, of course, ultimately ties to brand reputation and value, and attacks can mean a depreciation in brand for impacted hoteliers. According to past research from Ponemon's The Impact of Data Breaches on Reputation & Share Value, 71% of American CMOs believe the most significant cost of a security incident is brand value, which can affect companies for years after any cybersecurity event.

Consumers Are Most Concerned with Restaurant POS Vulnerabilities

Q: Which market's POS systems are most susceptible to cyberattacks?



Considering that 60% of restaurant breaches are caused by POS intrusions, it's not surprising that the majority of guests believe that restaurant POS systems are the most susceptible to cyberattacks across the hospitality industry (58%). The POS systems within sports and entertainment venues were next on consumer's lists (22%), followed by hotels (20%).

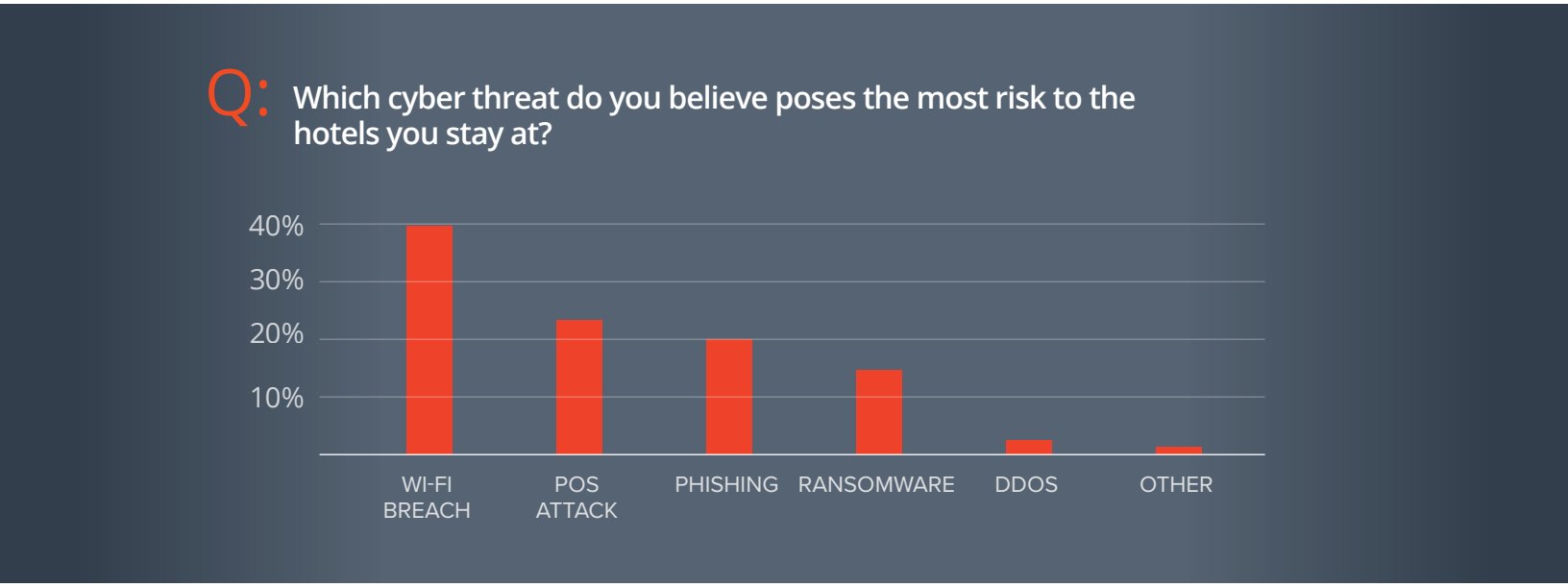
Increasingly attackers are targeting weakly defended point-of-sale systems as an entry point into the broader organizational network. With many POS devices in the hospitality industry still running on Windows 7 or even Windows XP-based embedded operating systems, they are increasingly vulnerable, and cybercrime groups are taking notice.

In addition to FIN8 targeting hospitality POS networks, Morphisec has tracked both FIN6 and FIN7 targeting this weak link. They are aided in their efforts by the fact that legacy antivirus is ineffective and many newer tools are too heavy to run on POS systems. Today's advanced attacks use multiple techniques to avoid detection — such as hijacking legitimate system resources to perform malicious actions — and can easily get past outdated and rudimentary POS defenses.

For instance, Buca di Beppo, Planet Hollywood and other Earl Enterprises' restaurant chains were all compromised by POS malware that resulted in the theft of more than 2 million customer credit and debit cards over a 10-month period.

POS malware is really a broader definition for an ever-expanding number of memory-scraper Trojans that are designed to scan for, grab and exfiltrate credit and debit card data from the endpoints that process and store it. Cybercriminals easily cash in this valuable information through dark web markets.

Guests Believe Compromised WiFi Poses the Biggest Risk at the Hotels They Stay at



While consumers believe restaurants have the hospitality industry's weakest POS system defenses, guests at hotels are far more worried about WiFi breaches by nefarious parties during their hotel stays. When asked what type of cyberattack they believe poses the biggest risk to the hotels they stay at, 40% of respondents noted a WiFi breach.

Part of this concern may be driven by a series of national stories this summer on "check-in" hacking tactics used by attackers to penetrate hotel systems. A Bloomberg article in June shed light on how cybercrime groups check into hotels themselves to gain access to hotel systems through WiFi networks as well as various weakly defended IoT devices.

While a large percentage of consumers are well-versed in the security weaknesses of hotel WiFi, the question remains if they are avoiding the risk by not logging on. If guests do decide to risk signing into hotel WiFi they should take some precautions. These include turning a laptop's firewall to block hackers and disabling sharing settings. Those conducting any sort of business activity or with sensitive information on their laptop should also look to use a Virtual Private Network (VPN).

The next biggest risk in the minds of consumers was a POS attack (23%), followed by phishing (20%) and ransomware (14%). While ransomware stories such as this one about hackers locking hotel guests out of their rooms have been exaggerated, ransomware is becoming an increasing threat to hotels and other hospitality businesses. A five-star hotel in India recently had its systems shut down by a ransomware attack. Perhaps more telling, the FIN6 cybercrime group, infamous for its hospitality and retail POS attacks, has branched out into deploying ransomware on infiltrated systems.

Conclusion

As the cyber threat to hospitality establishments continues, customers grow increasingly aware of security risks and make their travel plans accordingly. The best way organizations can protect their customer data and their brand is to build a strong preventative cybersecurity posture.

The hospitality industry has notoriously high employee turnover — make sure you have training programs in place to educate on the ways bad actors can get into your organization, such as phishing scams, adware, malware and viruses. Get rid of default passwords and make sure every staff member has their own login. Patch software regularly and keep security solutions up to date. Consider new, innovative prevention technologies that can stop advanced attacks but are lightweight enough for POS terminals.

ABOUT MORPHISEC

Morphisec has revolutionized endpoint protection with its Moving Target Defense technology, which instantly and deterministically stops the most dangerous and evasive attacks while allowing companies to cut operational costs. With a true prevention-first approach to stopping zero-days, with no false positives, Morphisec eliminates the complexity and burden for organizations struggling to respond to cyberattacks.

MORPHISEC
Moving Target Defense

www.morphisec.com