Trustwave®

Hospitality in the Crosshairs of Cybercrime

WHAT IS HAPPENING, WHY IS IT HAPPENING AND HOW YOU CAN RESPOND?

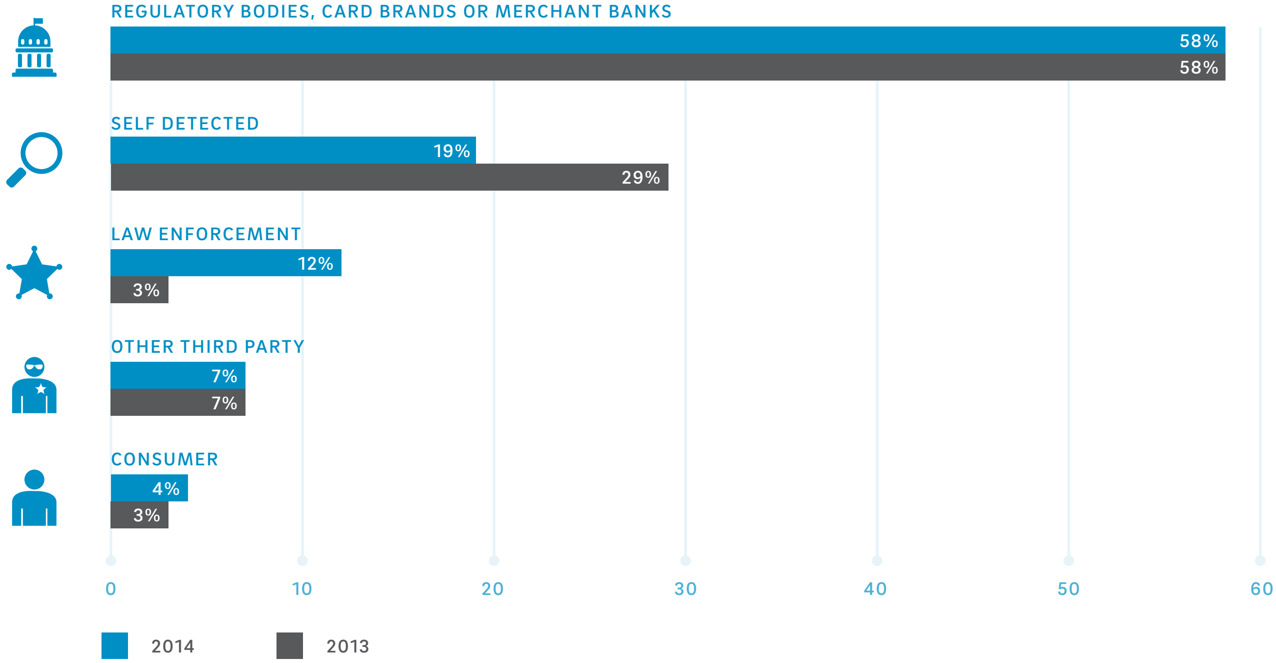
Overview

It's no surprise that cybercrime is accelerating across many industry sectors, but the hospitality industry is being increasingly targeted for a number of reasons – and it's not just for credit card data. Cybercriminals are finding a wealth of information within hotel systems that they can use to commit acts of fraud such as identity theft, rewards point theft and much more. There seems to be no end in the creative ways that organized crime syndicates are finding to monetize various pieces of valuable data. As a result, the attacks are continuing at record pace.

Cybercrime has made the move from pockets of targeted activities to full-time, highly sophisticated, persistent attacks that often linger for months, if not longer, and go largely undetected by the victim organization. In fact, according to the 2015 Trustwave Global Security Report, the median time that it takes an organization to detect compromise and subsequent breach was more than 100 days, and more than 80 percent of the time, the detection was not made by internal teams.

Mode Of Detection

Distribution of Trustwave forensic investigations by modes of detection in 2013 and 2014



So what exactly is going on here? Why is it happening? And arguably most importantly, how should hoteliers respond. Let's start by looking at a few of the more recent attacks and analyzing what took place to draw a baseline of current threat behaviors.

Recent Breach Analysis

No less than five major hotel groups and a hotel management firm confirmed data breaches at their properties nationally and internationally during 2015, during what may be considered the tip of the iceberg – with many more attacks to come. All of these compromises involved attack vectors that included point-of-sale systems at restaurants, gift shops and other on-property services that exposed the identities, rewards data and credit or debit card information of guests paying for such services. In at least one such compromise, a concession operator on the hotel property became a jumping-off point for further intrusions and attacks upon the host hotel. Below is a summary of the major activity during 2015.

- **Major Hotel Collection:** Confirmed a credit card breach following reports of a possible hack that was first publicized in July. The hack affected customers who used their credit or debit cards at several locations, including both national and international locations.
- **Global Hotelier:** Investigations were launched into a possible credit card breach at several of its properties, including the company's flagship locations, as well as many other branded hotels and resorts. Recently, their IT team confirmed the breach, citing unauthorized malware that targeted payment card information in some POS systems.
- **Major Hotel and Resort Chain:** Announced that hackers gained access to credit and debit card information of customers who dined or shopped at 54 of its hotels due to malware that infected POS systems in hotel gift shops, restaurants and stores. The breach did not occur at front desk payment systems, however.
- **Large Hotel Chain:** Recently announced that it had identified malware on some of its computer systems that process clients' payments, and has been working closely with leading cybersecurity experts to resolve the issue.
- **Major Global Hotel Chain:** The credit card systems at several hotels in the U.S. and Europe were hacked in 2015 with malware that infected sales systems at several properties, and revealed the personal information of guests who used credit or debit cards for dining, beverage, spa or other products and services. Many were U.S.-based properties, with London, Hong Kong, and Geneva locations also affected by the breach.
- **Hotel Management Firm:** Made public in 2015 a breach in data security, saying that 10 of the properties it manages were affected by attackers. Its POS systems at food and beverage outlets, such as hotel restaurants or lounges, sustained the malware attack. The hack affected two major brand families.

Threat Analysis

Although Trustwave was not involved in the investigation of all of the breaches outlined above, we were involved in a number of them and would offer the following specific commonalities about the nature of the threats involved and a few trends that we noticed in various other cases that we did investigate, which include;

- **Increased attacker sophistication:** POS environments are often targeted as a crime of opportunity, where simple exposed vulnerabilities are taken advantage to quickly steal card data. The recent trend in targeted hotel hacks – and some large-scale retailers – has shown an increased skill and persistence level. Attackers are targeting systems outside of the cardholder data environment and conducting advanced reconnaissance activity to laterally move throughout the network in search of segmentation weaknesses to target credit card data. Specifically, we are seeing third-party vendor access points being targeted, as they often are held to a lower security standard than corporate resources. This lateral traversal also allows attackers to drop backdoors on various points throughout the victim's network.
- **Varied Attack Vectors:** Beyond the insecure third-party access, we have also seen a focus on remote administration tools, such as LogMeIn, RDP and others, in addition to rudimentary phishing and drive-by download attacks that provide an initial inroad into the victim network. The attacker can laterally move from that point. The lateral attacker's job is often made easier by an obvious naming schema for POS systems. For example, when an attacker is enumerating the victim network, and they find a system within the cardholder environment named "POS1" or "MY-POS-VENDOR", it's a dead giveaway to target that particular POS system and makes the attackers job trivial.
- **Scaled-Down Polymorphic Malware:** Malware used in these attacks is often related to the major families that Trustwave already has discovered and analyzed, but attackers are frequently changing up their code to scale down the malware's functionality and cause it to change its structure upon each execution (polymorphism). The strategy behind this is to evade perimeter security systems and -software, as it appears to have been relatively successful in recent attacks.
- **Non-POS Attacks Also on the Rise:** While major POS breaches are hitting the headlines, we caution hotel clients not to focus only on that. 2015 also showed a rise in advanced persistent-type attacks targeting the personal information of hotel guests. Some nation-states are very interested in tracking the movements of certain executives and government officials, personal information, purchasing habits, and web surfing activity for intelligence-gathering purposes. The "Darkhotel" hacks from 2015 targeted vulnerable Wi-Fi points to compromise guest information for exactly this purpose.

Assessing Your Risk And Determining What To Do Next

Risk assessments are often the norm for operationalizing your security program. But many companies have gotten away from them and just began throwing technology at the problem – or focused exclusively on compliance frameworks like the PCI DSS. Obviously this isn't working, and in many cases has encouraged internal teams to focus solely on technology management and compliance, versus achieving true security.

A new, more streamlined approach to risk management is becoming a greater focus for many hospitality companies that have struggled to apply resources to the right areas and for the right reasons. Below is a brief quick summary of some of the key considerations that need to be followed to fully understand your risk profile and how to leverage that information more effectively throughout your data security programs and policies.

1. **Understanding where critical data lives within your enterprise and how it moves, both internally and outside of the organization.** This increasingly involves business partners and suppliers with whom data is shared because attackers can use them to gain a foothold into your network.
2. **Inventorying systems to understand their criticality, patch and vulnerability status.** This is really old-school advice, but still highly important none the less. The primary point here is to focus on key systems and data, not the entire infrastructure. Use advanced threat detection monitoring for watching the entire network for indicators of compromise.
3. **Evaluating key applications for vulnerabilities.** As additional services have been added for customers, such as mobile apps, you've also increased the size of your attack surface. In fact, Trustwave's experience in application testing found that 95 percent of mobile software we tested contained vulnerabilities and more than 98 percent of web-based applications also had vulnerabilities.
4. **Understanding current volumes of detected security incidents and how long it takes to respond to these known incidents.** In many cases, the information about a compromise is there, but it simply has been improperly categorized or missed completely. Security automation, analytics and a second set of eyes in the form of managed services are the key here to addressing this area.

Summary

We expect that the pace of attacks within the hospitality industry is going to continue to grow, and you need to focus in several key areas to avoid becoming the next breach headline. While the following list is not comprehensive, it offers our best advice in the context of how cybercriminals are operating within the hospitality space today.

1. Secure all third-party access points and ensure that they are following all of your corporate security rules, not just some of them.
2. Review POS segmentation and naming schema, and use a naming structure that does not indicate the system's purpose.
3. Increase employee awareness and training on standard drive-by downloads, phishing attacks, and other social engineering techniques.
4. Conduct higher-tier penetration testing on both general network environments and individual hotel Wi-Fi environments. The basic PCI pen test may not be enough to accurately give you an idea of vulnerabilities within your network
5. Ensure that your Incident Response Plan is efficient, effective and tested. Run attack simulations to ensure your security team is following and is trained on the plan.
6. Have an expert IR/forensic/malware reverse engineering team from a managed security services provider ready to respond in the event of an attack.

Finally, you don't have to go it alone. Partnering with an MSSP like Trustwave can offer you the edge you need to stay out of the headlines. We operate on a global scale with tremendous experience within the hospitality industry and very likely have already seen and dealt with the type of attack you might experience, so there is no delay or opportunity for the attackers to become embedded within your operations. An experienced, expert support team can make all the difference in the world when it comes to both recognizing and responding to today's advanced threats. Give Trustwave a call today!

https://www.trustwave.com/services

Trustwave®

For more information: www.trustwave.com