UNIVERSITY OF WEST LONDON
The Career University

UWL REPOSITORY

repository.uwl.ac.uk

Cyber risk resilience quarterly : threat intelligence for hotel, restaurants and tourism sectors. Q3 2026.

Paraskevas, Alexandros ORCID logoORCID: https://orcid.org/0000-0003-1556-5293 (2026) Cyber risk resilience quarterly : threat intelligence for hotel, restaurants and tourism sectors. Q3 2026. Technical Report. University of West London, London.

This is the Draft Version of the final output.

UWL repository link: https://repository.uwl.ac.uk/id/eprint/15791/

Alternative formats: If you require this document in an alternative format, please contact: open.research@uwl.ac.uk

Copyright:

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy: If you believe that this document breaches copyright, please contact us at open.research@uwl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Rights Retention Statement:

UNIVERSITY OF WEST LONDON
The Career University

CYBER RISK & RESILIENCE QUARTERLY

Threat Intelligence for Hotel, Restaurant, Tourism and Aviation Sectors

Q3 2026

ICHARM
International Center for Hotel and Aviation Resilience Management

Welcome from the Dean



James Edmunds

Dean, London Geller College of Hospitality & Tourism

Welcome to the third edition of the Cyber Risk and Resilience Quarterly. This edition covers incidents affecting hotels, restaurant and food service operators, tourism businesses, aviation organisations and the technology suppliers that directly support them between July and September 2026. After the exclusions applied during the research stage, the report records 99 incidents during the quarter and 13 earlier attacks that became public during Q3.

The number is much higher than in the first two editions, but it should not be read as a simple quarter-on-quarter increase. Aviation is included as a full sector for the first time and the Q3 research used wider leak-site coverage. What does stand out is the weight of ransomware and data-extortion claims, together with a smaller number of confirmed incidents that caused serious operational disruption or exposed very large customer datasets.

Manchester Airports Group disclosed a breach affecting about 8.8 million customer records. Hit in Slovenia closed six casinos for about three days. Times Car in Japan disclosed about 6.6 million affected accounts. These cases show the same problem from different directions: data loss, service interruption and regulatory exposure can develop from the same incident.

The sections that follow examine the incidents, the methods used and the groups responsible and conclude with practical recommendations for managers and security teams.

A Note from the Researcher

In Q1 the weak point was identity. In Q2 it was the platform. Q3 is harder to reduce to one failure because the quarter is dominated by scale. There are more extortion claims, more large datasets and more cases where a single supplier, exposed secret or customer-facing service can affect many organisations or millions of customers.

Manchester Airports Group is the clearest case. An API key exposed in website code was linked to the theft of customer data. The group refused the ransom demand, and the stolen material was published. The incident did not need sophisticated malware or a long intrusion to create a breach of this size.

Other cases widened the picture. An AI-driven skimming campaign placed card-stealing code on at least 119 websites and was reported to have taken more than 600,000 card records from two unnamed companies, one in hospitality and one in aviation. A rogue Wi-Fi network appeared on a Delta flight. IDScan.net disclosed the theft of identity-document scans used by businesses including bars, venues and car-rental counters.

There is also a problem with the evidence. Seventy-nine of the 99 Q3 incidents in scope are based on threat-actor claims that had not been independently confirmed by the research cut-off. A leak-site listing tells us that a criminal group is applying pressure. It does not, by itself, prove that the organisation was breached or that the data shown is genuine.

We hope the information in this report helps managers and cybersecurity teams protect their organisations against these methods.



Prof. Alexandros Paraskevas

Chair in Hospitality Management & Director, ICHARM

Contents

Executive Summary **4**

1. Incident Chronology **5**

1.1 Incident Timeline 5

1.2 Incident Analysis 10

1.3 Key Findings for Q3 2026 10

2. Incident Overview **12**

2.1 How the Attacks Unfolded 12

2.2 Sector Summary 12

3. Threat Actor Profiles **14**

3.1 The Threat Actor Landscape 14

3.2 Adversary Behaviour Patterns 14

4. Cyber Threat Trends **15**

Trend 1. Data extortion is now the default public threat signal 15

Trend 2. Leak Site volume is outpacing verification 15

Trend 3. Public-facing secrets can create enterprise breaches 15

Trend 4. Identity datasets are becoming sector infrastructure 15

Trend 5. Customer interaction channels are attack surfaces 15

Trend 6. Operational disruption is back in the picture 15

Trend 7. Supplier compromise remains a multiplier 15

5. Tactics, Techniques and Procedures **16**

5.1 Leak Site extortion and publication pressure 16

5.2 Exposed API keys and secrets 16

5.3 Ransomware with operational disruption 16

5.4 Exploitation of third-party software 16

5.5 Web skimming and autonomous tooling 16

5.6 Rogue Wi-Fi and deceptive customer interfaces 16

5.7 Cloud and identity-data theft 16

5.8 Booking and customer-platform compromise 16

5.9 Data resale and downstream fraud 16

6. Sector Specific Risk Profiles **17**

6.1 Hotels 17

6.2 Restaurants and Food Service 17

6.3 Tourism and Travel 17

6.4 Aviation 17

6.5 Cross-Sector Observations 18

7. Monetisation **19**

7.1 How Attackers Convert Breaches into Revenue 19
7.2 Ransom Demands and Cryptocurrency 19
7.3 The Decision to Pay or Refuse 19
7.4 Leak Site Pressure and Data Publication 19
7.5 Loyalty and Identity Exploitation 19
7.6 Insurance and Post-Breach Costs 19
8. Legal, Regulatory and Litigation Landscape 20
8.1 Litigation and Notification Exposure 20
8.2 Sector Regulatory Tracker 20
8.3 Cyber Insurance 20
9. Threat Outlook 21
9.1 Ransomware and Data Extortion 21
9.2 Identity and Credential Exploitation 21
9.3 Third Party and Supply Chain Risk 21
9.4 Social Engineering Targeting Sector Staff 21
9.5 Web Skimming and Customer-Facing Malware 21
9.6 Regulatory and Litigation Pressure 21
9.7 Operational Technology and Physical Systems 21
9.8 Insider Threats 21
9.9 Monetisation and Dark Web Activity 21
Assessment Summary 21
10. Recommendations 22
10.1 Secret and API Key Governance 22
10.2 Ransomware and Data-Extortion Readiness 22
10.3 Supplier, Booking and Platform Assurance 22
10.4 Customer-Facing Web, Payment and Wi-Fi Monitoring 22
10.5 Aviation Operational Resilience 22
10.6 Data Minimisation and Segmentation 22
10.7 Tabletop Exercise Scenarios for Hotel, Restaurant, Tourism and Aviation Environments 23
Endnotes 24
Appendix A. Full In-Scope Incident Matrix 26
Appendix B. Detailed Threat Actor Profiles 40

Executive Summary

The third quarter of 2026 produced a much larger incident set than the first two editions. After removing the peripheral sectors identified during the research stage, this report records 99 incidents between 1 July and 30 September across hotels, restaurant and food service, tourism, aviation and directly connected technology suppliers. A further 13 earlier attacks became public during the quarter. The figures are not directly comparable with Q2 because aviation is now included as a full sector and the leak-site coverage is wider.

The underlying pressure still rose. Check Point Research recorded an average of 2,614 weekly attacks per organisation in hospitality, travel and recreation during July, up 28% year on year. In August the figure reached 3,056, up 56%, and the sector moved to third place among the industries covered by the research.[3,4]

Ransomware and data extortion account for most of the quarter. Seventy-nine of the 99 incidents rest on threat-actor claims that had not been independently confirmed at the research cut-off. This is an important distinction. A leak-site listing shows criminal activity and pressure against a named organisation, but it does not establish the date of intrusion or prove that the claimed data was taken.[5]

The largest confirmed data incident was Manchester Airports Group. About 8.8 million records linked to Manchester, London Stansted and East Midlands airports were reported affected. The data included email addresses, telephone numbers, vehicle registrations, postcodes and bookings for parking, lounges and Fast Track. The stolen material was published after the company refused the ransom demand.[6,7,8,9]

Operational disruption also returned. Hit in Slovenia closed six casinos for about three days, with hotel reception, cash registers and the loyalty system affected. Keio Group in Japan partly shut down networks and reported disruption to hotel communications and reservations. These were not simply privacy incidents. They interrupted the services customers and staff use every day.[10,20]

Large identity datasets remained a target. IDScan.net disclosed the theft of driving-licence scans used across customer-verification environments. Times Car reported about 6.6 million current and former user accounts affected. Aeromexico investigated a dataset advertised as holding more than 15 million customer records, although the origin and age of that material had not been established at the cut-off.[12,19,21]

Two methods deserve attention because they sit outside the usual picture of ransomware. An AI-driven skimming campaign was reported to have placed card-stealing code on at least 119 websites and taken more than 600,000 card records from two unnamed companies, one in hospitality and one in aviation. On a Delta flight, a passenger broadcast a false Wi-Fi network that looked like an airline service. Both attacks reached customers through services they expected to trust.[11,13]

Six findings matter most for managers:

- API keys, tokens and other secrets exposed in public-facing code should be treated in the same way as passwords.
- Data extortion can continue even when systems are available and backups are intact.
- A supplier or booking-platform breach can create notification and customer-service obligations for the operator even when its own network was not compromised.
- Websites, payment pages and guest or passenger Wi-Fi now need the same monitoring discipline as internal systems.
- Leak Site claims and confirmed incidents should be reported separately to boards, insurers and regulators.
- Continuity plans need to cover reservations, reception, payments, loyalty and aviation services as well as data recovery.

1. Incident Chronology

The third quarter produced far more public incident reports and leak-site listings than Q2. This chronology therefore uses a selective set of confirmed, high-impact and representative cases. The full in-scope register appears in Appendix A. Where the attack date is known, that date is used. For leak-site claims, the date is the date of listing and will usually be later than the intrusion itself.

1.1 Incident Timeline

Date	Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status
1 Jul 2026	Refinery Hotel (USA)	Hotel	Akira	Ransomware and data extortion	15 GB claimed, including employee passports, driving licences and Social Security numbers, guest information and contracts	Claimed by threat actor (unconfirmed)
13 Jul 2026	BE Travel (ZA)	Tourism and Travel	Arcus Media	Ransomware	Travel voucher and administration system for a government agency; personal information may have been accessed or encrypted; POPIA notifications issued	Confirmed by victim
Late Jul 2026 (claim 28 Jul)	accesso Technology Group (UK)	Sector technology	Coinbase Cartel	Unauthorised access and data theft	Ticketing and queuing software for attractions; limited systems accessed, no downtime; group claims internal files	Confirmed by victim
31 Jul 2026	THY, Turkish Airlines (TR)	Aviation	CRPxO	Data extortion	Flag carrier listed; 4.2 GB claimed	Claimed by threat actor (unconfirmed)
13 Jul 2026	Nichirei (JP)	Restaurant and Food Service	RansomHouse	Unauthorised access and data extortion	Cold storage and logistics failure disrupted frozen food supply to about 5,000 partners including KFC Japan and Kura Sushi; employee and partner data later published	Confirmed by victim
Jul to Sep 2026	AI driven skimming campaign, unnamed Fortune 500 hospitality	Aviation	Unattributed, Chinese speaking operator (Gambit)	Web skimming by autonomous AI agents	At least 119 sites carried card skimmers; more than 600,000 card records	Under investigation

Date	Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status
	company and major US airline (USA)				stolen from two firms; campaign active July to at least 22 September	
3 Aug 2026	TUI China (CN)	Tourism and Travel	DragonForce	Ransomware and data extortion	Passports, visas, internal, legal and financial documents claimed	Claimed by threat actor (unconfirmed)
6 Aug 2026	Woodhaven Lakes (USA)	Tourism and Travel	Play (claim)	Ransomware and data theft	Private recreational resort; phones, payments and facilities disrupted; local files encrypted, off-site backups intact; property owner database reportedly not breached	Confirmed by victim
Aug 2026 (listed 12 Aug)	Toast (USA)	Sector technology	Cl0p	Data theft through PTC Windchill flaw (CVE-2026-12569)	Restaurant POS provider named; 215 GB of project, backup database and log data claimed	Claimed by threat actor (unconfirmed)
9 Aug 2026	Mikel Coffee (GR)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Chain of 410 stores in 19 countries; customer contact and password data claimed; no sample released	Claimed by threat actor (unconfirmed)
10 Aug 2026	Delta Air Lines Flight 591 (USA)	Aviation	Unattributed passenger	Rogue Wi-Fi access point	Fake network called Delta WiFi Fast broadcast in flight; crew disabled onboard Wi-Fi for about 30 minutes; FBI aware	Confirmed by victim
24 Aug 2026	Furnished Quarters (USA)	Hotel	Dark Project	Data theft and extortion	155 GB and about 198,000 files claimed, including customer, banking and financial data	Claimed by threat actor (unconfirmed)
Overnight 24 to 25 Aug 2026 (Akira claim 23 Sep)	Hit d.d. (SI)	Tourism and Travel	Akira (claim 23 Sep)	Ransomware	Six casinos closed for about three days; hotel reception, cash registers and loyalty system disrupted; 367	Confirmed by victim

Date	Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status
					GB claimed including employee IDs and client data	
Aug 2026 (disclosed 25 to 27 Aug)	Manchester Airports Group (UK)	Aviation	FulcrumSec	API key exposed in website code, data theft and extortion	About 8.7 million customer records from Manchester, Stansted and East Midlands, revised to about 8.8 million by Have I Been Pwned; emails, phone numbers, vehicle registrations, postcodes, parking, lounge and Fast Track bookings; 86 GB claimed; data published 2 to 3 Sep after ransom refusal; ICO assessing	Confirmed by victim
27 Aug 2026	Hungry Lion (ZA)	Restaurant and Food Service	MedusaLocker	Ransomware and data extortion	Point of sale data from Unity, GAAP and CoSoft systems posted; USD 50,000 demand; no customer personal data seen in samples	Claimed by threat actor (unconfirmed)
Discovered 1 Sep 2026	IDScan.net (USA)	Sector technology	Unattributed, sold through Nexus marketplace	Cloud data theft over about a year	More than 153 million US and Canadian driving licence scans offered; used by bars, venues and car rental counters; FBI investigating	Confirmed by victim
4 Sep 2026	Toronto Pearson, GTAA (CA)	Aviation	Unattributed	Social media account hijack	Airport X account briefly hijacked for crypto promotion; operations and security systems unaffected	Confirmed by victim
5 Sep 2026	The Big Table Group (UK)	Restaurant and Food Service	Qilin	Ransomware and data extortion	Operator of Bella Italia, Café Rouge and Las Iguanas listed	Claimed by threat actor (unconfirmed)
14 Sep 2026	Atlas Ocean Voyages (USA)	Tourism and Travel	Booba Project	Data extortion	Expedition cruise line listed; 37 GB claimed	Claimed by threat actor (unconfirmed)

Date	Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status
15 Sep 2026	EVA Airways (TW)	Aviation	Unattributed	Unauthorised network access	Internal network infiltrated via suspicious IPs; employee names and business contacts accessed; operations unaffected; disclosed through TWSE	Confirmed by victim
15 Sep 2026	Evergreen Aviation Technologies (TW)	Aviation	Unattributed	Cyberattack on internal systems	Maintenance provider; endpoints isolated, core operations normal; data impact undisclosed	Confirmed by victim
24 Sep 2026	Ligue-se Grupo (PT)	Sector technology	The Gentlemen	Ransomware and data extortion	Madeira IT group supplying hotel technology listed	Claimed by threat actor (unconfirmed)
18 Sep 2026	Atlantic Hotels Group (DE)	Hotel	Unattributed	Website compromise (ClickFix)	Atlantic, SEVERIN*S and unique by ATLANTIC hotel websites served a fake Cloudflare check that pushed PowerShell malware to visitors; sites offline until 21 Sep; company says no guest or company data stolen	Confirmed by victim
18 Sep 2026	Aeroméxico (MX)	Aviation	Unattributed, advertised on Telegram	Data theft, origin unclear	Database of 1.1 GB with more than 15 million customer records advertised, sample including public officials; ministry probe opened; airline found no card or password evidence; possibly recycled October 2025 data	Under investigation
Disclosed 18 to 23 Sep 2026	Maritim Hotels via Amadeus iHotelier (DE)	Hotel	Unattributed	Third-party reservation platform breach	8,716 guests notified; stays 1 Aug 2026 to 30 Sep 2027; postal addresses, emails and phone	Confirmed by victim

Date	Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status
					numbers; no payment or passport data	
Detected 25 Sep 2026	Times Mobility, Times Car (JP)	Tourism and Travel	Unattributed	Unauthorised access to web systems	About 6.6 million current and former car sharing and rental accounts plus corporate accounts, including 1.6 million identity verification records such as driving licence images; access from early Sep, theft confirmed 28 Sep; card data not affected; reported to PPC and police; Park24 group company	Confirmed by victim
26 Sep 2026	Keio Group, Keio Plaza Hotel (JP)	Hotel	Unattributed	Ransomware	Group networks partly shut down; hotel communications and reservation processes disrupted; trains ran normally; customer data exposure under investigation	Confirmed by victim
Not stated (disclosed 26 Sep 2026)	Air Traffic and Navigation Services (ZA)	Aviation	Unattributed	Ransomware, possible insider involvement	Operational technology for weather related air traffic services hit; possible exfiltration to IP addresses in China; forensic tender issued	Under investigation
Discovered 26 Sep 2026	Starts Publishing, OZmall (JP)	Sector technology	Unattributed	Unauthorised access from overseas	Restaurant, hotel and salon booking platform; up to 442,779 email addresses, some with names and prefecture; no cards or passwords; reported to PPC 28 Sep	Confirmed by victim
29 Sep 2026	Camp Ozark, Ozark Interests (USA)	Tourism and Travel	Unattributed	Data breach	Names, addresses, bank and payment card data; Texas	Disclosed via breach notification

Date	Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status
					attorney general filing	

1.2 Incident Analysis

Data extortion at scale

Data theft followed by a threat to publish was the most common pattern in Q3. The Gentlemen produced the largest number of in-scope sector listings, followed by Qilin. In many cases the public record contains little more than the name of the victim and the group's claim. This gives a clear picture of extortion activity, but a much weaker picture of how the attackers actually got in.[1,2,5]

Manchester Airports Group shows what happens when the claim is supported by a confirmed disclosure. An API key exposed in website code was linked to access to customer data. The company refused the ransom demand and the data was then published. A secret left in public code became the entry point to a breach affecting millions of records.[7,8,9]

Operational disruption returned

Hit in Slovenia was the clearest operational case. Six casinos were closed for about three days and hotel reception, cash registers and loyalty functions were affected. Keio Group also reported disruption to hotel communications and reservation processes. Q2 was dominated by data held outside the organisation. Q3 brings availability back into the picture.[10,20]

Third-party and platform dependence

Several incidents began with systems operated by somebody else. Maritim Hotels notified guests after an incident involving Amadeus iHotelier. Starts Publishing disclosed unauthorised access affecting the OZmall booking platform. accesso Technology reported limited unauthorised access to systems supporting attractions. Toast was named in the Cl0p campaign linked to a PTC Windchill vulnerability, although there was no evidence that restaurant customer data was exposed.[16,24]

Customer identity and verification data

IDScan.net shows the concentration risk created by identity-verification services. The material offered for sale was reported to include more than 153 million US and Canadian driving-licence scans. Hotels, venues and travel businesses often outsource this kind of verification precisely because they do not want to hold the documents themselves. The data risk does not disappear when the storage is moved to a supplier.[12]

New customer-facing attack surfaces

The AI skimming campaign and the Delta Wi-Fi incident both attacked the customer-facing layer. One placed malicious code on websites. The other presented passengers with a false wireless network. In neither case did an attacker need to break into the organisation's internal network first.[11,13]

1.3 Key Findings for Q3 2026

99 in-scope incidents are recorded for Q3 after the agreed exclusions, plus 13 earlier attacks disclosed or claimed during the quarter.

Hotels account for 27 incidents, tourism and travel for 26, restaurant and food service for 22, aviation for 19 and directly connected technology suppliers for 5.

Seventy-nine of the 99 Q3 incidents are unconfirmed threat-actor claims. This is the main limitation of the evidence.

Manchester Airports Group is the largest confirmed customer-data exposure in the Q3 set, at about 8.8 million records.

Operational disruption affected casinos, hotel reservations and communications, and aviation-related environments. Incident response therefore needs a continuity plan as well as a data-breach plan.

An API key exposed in public website code was linked to an enterprise-scale breach. Secrets in code need the same controls as user credentials.

Booking, ticketing, point-of-sale and identity-verification suppliers remain part of the sector's attack surface.

Customer-facing websites and Wi-Fi are now direct targets, including AI-assisted skimming and rogue-network techniques.

Passports, driving licences, loyalty accounts and travel records continue to carry high regulatory and fraud exposure because they are difficult or impossible for the customer to replace.

2. Incident Overview

Q3 contains two very different types of evidence. A smaller group of confirmed incidents shows what happened and what the consequences were. A much larger group of leak-site claims shows where criminal groups are applying pressure, but often tells us very little about the intrusion itself. The two should not be treated as equivalent.

2.1 How the Attacks Unfolded

Initial Access - how attackers got in

Public reporting established the initial access route in only a small number of cases. Manchester Airports Group was linked to an API key exposed in website code. Toast appeared in the Cl0p campaign against PTC Windchill. Atlantic Hotels websites served a fake Cloudflare check. A Delta flight carried a false Wi-Fi access point. These are very different routes, but all begin outside the traditional corporate perimeter.[7,13,18,24]

Execution and Persistence - what ran and how it stayed

Ransomware was the clearest execution method in the incidents that caused disruption. In many of the extortion claims, however, it is not known whether anything was encrypted. The AI skimming campaign used malicious code on websites rather than an endpoint payload. For most leak-site claims, execution and persistence were simply not reported.[11]

Credential Access and Evasion - how attackers used trusted access

Q3 provides less direct evidence on credential theft than Q2. What it does show is that attackers can use exposed secrets, legitimate external access and third-party platforms without producing the signals associated with conventional malware. Access logs and inventories of keys and tokens therefore matter as much as endpoint alerts in these cases.

Collection and Exfiltration - what attackers took

The high-impact incidents centred on personal data: contact details, booking information, driving-licence scans, loyalty records and travel data. Criminal claims also advertised employee, contract and financial material. Data becomes more useful to an attacker when identity is combined with travel or service information because the resulting fraud is much easier to make convincing.

Impact - what it cost the organisations

Consequences ranged from no reported downtime to closures lasting several days. Reservation, communication, loyalty and payment functions were affected in confirmed cases. Manchester Airports Group continued operating, but publication of the stolen data after ransom refusal created a separate regulatory and customer burden. Availability and confidentiality produced different costs, but both required senior management attention.[7,9,10,20]

2.2 Sector Summary

Sector	Q3 Incidents	Confirmed / disclosed	Unconfirmed claims	Typical exposure	Operational examples
Hotel	27	3	24	Guest and employee data; reservation systems; web content	Keio Plaza reservation and communications disruption
Restaurant and Food Service	22	1	21	Loyalty, POS, employee and internal business data	Nichirei supply disruption; Hungry Lion POS data claim

Sector	Q3 Incidents	Confirmed / disclosed	Unconfirmed claims	Typical exposure	Operational examples
Tourism and Travel	26	5	21	Booking, identity, payment and loyalty data	Hit casino closures; Times Car account exposure
Aviation	19	8	11	Airport bookings, passenger and employee data; operational services	MAG data publication; Delta rogue Wi-Fi; ATNS investigation
Sector technology	5	3	2	Booking, ticketing, POS and identity-verification platforms	accesso, IDScan, OZmall and Toast exposure

3. Threat Actor Profiles

3.1 The Threat Actor Landscape

The threat-actor set is broader than in Q2 and more fragmented. The Gentlemen produced the largest number of in-scope listings, followed by Qilin. Several groups appeared only once or twice and ten incidents were recorded as unattributed. Frequency should not be confused with impact. FulcrumSec appears only once in the Q3 dataset, but that single case is the Manchester Airports Group breach.

Threat Actor	Q3 In-scope listings	Preferred pattern	Sector evidence	Assessed risk
The Gentlemen	16	Ransomware and data extortion; high-volume leak-site listing	Restaurant and food service, aviation, hotel and sector-technology targets	Critical
Qilin	9	Ransomware and data extortion; repeated sector listings	Hotels, restaurants and tourism businesses	Critical
Krybit	5	Ransomware and data extortion	Multiple hotel and aviation claims	High
Settra	4	Data extortion	Tourism and hotel claims	High
DragonForce	4	Ransomware and data extortion	Tourism, hotels and restaurants	High
Akira	3	Ransomware and data extortion	Refinery Hotel and Hit; major operational disruption at Hit	High
FulcrumSec	1	Data theft and extortion linked to an exposed API key	Manchester Airports Group	Critical

3.2 Adversary Behaviour Patterns

Volume creates uncertainty as well as pressure

Leak sites are now part of the pressure campaign, not just a place where stolen data is published at the end. Four in every five Q3 incidents in the dataset are unconfirmed claims. A company can therefore face media questions, supplier concerns and board attention before it knows whether anything was taken. The first response has to separate the criminal claim from the evidence available internally.[5]

Data publication is part of the extortion model

Manchester Airports Group gives the clearest sequence: data was taken, a demand was made, the company refused and the material was published. Backups do not solve this kind of incident because the attacker is not relying on keeping systems locked. The leverage is the disclosure of the data itself.[7,9]

Attackers follow concentrated data

Shared services remain attractive because they concentrate data. Identity verification, booking and customer platforms can give an attacker access to records belonging to many users or organisations at once. IDScan.net, Amadeus iHotelier, OZmall and the sector-technology cases in this edition all show the same concentration effect.[12,16]

4. Cyber Threat Trends

Trend 1. Data extortion is now the default public threat signal

Ransomware and data extortion dominate the Q3 record. In many of the leak-site cases the public evidence is limited, but the criminal model is consistent: take data, set a deadline and threaten publication. Managers should therefore prepare for an extortion incident even when systems are still working.

Trend 2. Leak Site volume is outpacing verification

Seventy-nine of 99 Q3 incidents are unconfirmed threat-actor claims. The volume matters because every listing can trigger investigation and communications work. It should not be used as a count of successful intrusions.

Trend 3. Public-facing secrets can create enterprise breaches

The Manchester Airports Group case shows how an exposed API key in website code can lead to a major breach. Keys, tokens and other secrets should not appear in client-side code, and they should be scanned for, restricted and rotated in the same way as passwords.

Trend 4. Identity datasets are becoming sector infrastructure

Driving-licence scans, passenger records, loyalty accounts and booking histories are increasingly held in shared services. One failure can therefore reach customers across many businesses and jurisdictions.

Trend 5. Customer interaction channels are attack surfaces

The AI skimming campaign and the false Delta Wi-Fi network both targeted the service the customer was using directly. Websites, booking journeys and guest or passenger connectivity can be compromised even when the organisation's internal systems continue to work normally.

Trend 6. Operational disruption is back in the picture

Hit and Keio show that reception, reservations, cash registers, loyalty and communications can still be interrupted. Q3 therefore brings business continuity back alongside data-breach response.

Trend 7. Supplier compromise remains a multiplier

Booking, ticketing, point-of-sale and identity-verification suppliers appear repeatedly in the Q3 evidence. Operators cannot patch a supplier's systems themselves, but they can decide what data the supplier receives, how quickly an incident must be reported and how the organisation will operate when the service is unavailable.

5. Tactics, Techniques and Procedures

5.1 Leak Site extortion and publication pressure

The most common extortion pattern is simple. A group names the victim, posts a deadline or sample and threatens publication. The incident team then has to establish whether the claim is genuine, decide what needs to be reported and manage communications at the same time.

5.2 Exposed API keys and secrets

API keys, tokens and credentials can give direct access to data when they are left in public code or configuration. Keep them outside client-side applications, scan for them automatically, restrict what each key can reach and rotate it as soon as exposure is suspected.

5.3 Ransomware with operational disruption

When ransomware does interrupt systems, recovery has to follow the business process rather than the server list. Reception, reservations, payments, loyalty and communications may all need manual alternatives before the technical rebuild is complete.

5.4 Exploitation of third-party software

The Cl0p campaign involving PTC Windchill shows why widely used enterprise software remains attractive. One flaw can create a route to many organisations. Operators need to know which externally exposed products their suppliers use and how quickly those suppliers patch serious vulnerabilities.

5.5 Web skimming and autonomous tooling

The Q3 skimming campaign was reported to use AI-driven agents to place card-stealing code on websites. The new element is the automation, not the underlying control problem. Changes to payment pages, third-party scripts and externally loaded code need to be monitored whether the attacker uses AI or not.[11]

5.6 Rogue Wi-Fi and deceptive customer interfaces

A false Wi-Fi network can look close enough to the genuine service for a guest or passenger to use it. Hotels, airports and airlines should publish the exact network name, look for unauthorised access points and make sure front-line staff know where to report a suspicious network.[13]

5.7 Cloud and identity-data theft

Identity documents have a long life. A password can be changed and a payment card can be replaced; a driving licence or passport number is much harder to deal with once it is exposed. Keep these records only for as long as they are needed and apply the same access controls to a supplier repository as to an internal one.

5.8 Booking and customer-platform compromise

The Maritim Hotels and OZmall incidents show how closely booking platforms sit between the customer and the operator. Contracts should say how quickly the supplier must notify the organisation, what investigation evidence will be shared, how affected customers will be identified and who will contact them.

5.9 Data resale and downstream fraud

The breach does not necessarily end when the attacker leaves. Stolen booking or identity data can be sold, reused for impersonation or used in convincing follow-up fraud. Customer warnings and monitoring for secondary abuse should therefore form part of the response.

6. Sector Specific Risk Profiles

6.1 Hotels

Hotels account for 27 Q3 incidents in scope. Many are ransomware or extortion claims, but the confirmed cases are more useful for understanding where the exposure sits. Atlantic Hotels websites served a fake Cloudflare check. Maritim Hotels notified guests after an Amadeus iHotelier incident. Keio Group reported disruption affecting hotel communications and reservation processes.[18,20]

The lesson for hotel operators is that the property management system is only one part of the environment. The website, booking engine, guest communications and supplier integrations can all expose guests or interrupt service even when the PMS itself is unaffected.

Data Assets at Risk

Data Asset	Q3 Exposure
Guest identity and contact data	Names, addresses, emails, telephone numbers and booking details appeared in confirmed and claimed incidents.
Reservation data	Third-party booking platforms can expose future stays and customer contact information.
Employee data	Passports, identity documents, HR and internal business records were repeatedly claimed.
Website trust	Fake verification pages and malicious web content can target guests before they reach internal systems.
Loyalty and payment context	Loyalty, cash register and payment-related systems featured in operational disruption and extortion claims.

6.2 Restaurants and Food Service

Restaurant and food service operators account for 22 Q3 incidents after food manufacturers are removed. The Gentlemen produced the largest share of claims in this subsector. Mikel Coffee, KFC Kosova and The Big Table Group appeared on leak sites. Hungry Lion was linked to a USD 50,000 demand and samples involving point-of-sale data, although the claim remained unconfirmed at the research cut-off.[14,15]

Card data is only part of the exposure. Loyalty accounts, staff records, supplier information, internal finance and point-of-sale configuration can all be used for extortion or follow-on fraud. Chains and franchise systems also need to account for uneven local technology and support arrangements.

6.3 Tourism and Travel

Tourism and travel account for 26 Q3 incidents after the agreed exclusions. Hit in Slovenia was the most disruptive confirmed case: six casinos closed for about three days and hotel reception, cash registers and loyalty systems were affected. Times Car later disclosed about 6.6 million current and former customer accounts. Atlas Ocean Voyages was listed with 37 GB claimed, but that claim was not independently confirmed.[10,19]

Travel businesses hold data that can remain useful to a criminal for years: identity details, itineraries, loyalty information and booking history. Keeping less of it, and separating booking, loyalty and payment systems, limits what one compromised service can expose.

6.4 Aviation

Aviation is included as a full sector in this edition and accounts for 19 Q3 incidents. Manchester Airports Group is the largest confirmed data case. Other incidents include a false Wi-Fi network on a Delta flight, confirmed

unauthorised access at EVA Airways, an investigation into an Aeromexico dataset and an investigation involving South Africa's Air Traffic and Navigation Services.[7,9,13,21,23]

Aviation combines large passenger datasets with services that cannot tolerate long outages. The Q3 cases span airport commercial systems, airline customer platforms, catering and support suppliers, and air-navigation functions. The resilience problem therefore extends well beyond the airline's corporate network.

6.5 Cross-Sector Observations

Third-party platforms can create the widest exposure because they hold data or provide services for many organisations at once.

Data theft can be as costly as encryption when the stolen material is published or reused against customers.

Operational continuity still matters even though most Q3 criminal claims are about data rather than system encryption.

A leak-site claim, a victim confirmation and a regulatory filing are different levels of evidence and should be reported as such.

Websites, booking engines, Wi-Fi and identity-verification services should be treated as production systems, not as peripheral digital services.

7. Monetisation

7.1 How Attackers Convert Breaches into Revenue

Q3 shows four routes to revenue: ransom or extortion demands, pressure through threatened publication, resale of stolen customer or identity data, and secondary fraud using booking, loyalty or payment information. The same breach can support more than one of these, which means restoring encrypted systems does not necessarily end the incident.

7.2 Ransom Demands and Cryptocurrency

Very few ransom figures became public during Q3. Hungry Lion was associated with a USD 50,000 demand in the threat-actor claim. Manchester Airports Group refused a demand and the stolen data was later published. In the other cases, the amount under discussion, if any, was not disclosed.[7,14]

7.3 The Decision to Pay or Refuse

There is not enough public evidence to say how often organisations paid during Q3. The Manchester Airports Group case does show one consequence of refusal: publication of the stolen data. The decision therefore needs to be worked through in advance with legal, insurance and operational teams rather than improvised against a criminal deadline.[7,9]

7.4 Leak Site Pressure and Data Publication

A leak-site listing creates pressure whether the claim is genuine or not. The organisation may have to answer media, customer and partner questions before the technical investigation is complete. The response should preserve the listing, test any sample data, check the logs and state clearly what has and has not been confirmed.

7.5 Loyalty and Identity Exploitation

Loyalty and identity records retain value after the original breach because they can support account takeover, impersonation and targeted scams. The Q3 incidents involving driving licences, loyalty accounts and travel data make retention limits and prompt customer warnings more important.[12,22]

7.6 Insurance and Post-Breach Costs

The Q3 research does not provide enough evidence to compare cyber-insurance prices or policy terms across the sector. It does show the costs that need to be covered: forensic work, legal advice, notification, customer support, restoration, business interruption, supplier disputes and extortion response. These costs arise even where nothing was encrypted.

8. Legal, Regulatory and Litigation Landscape

8.1 Litigation and Notification Exposure

The main legal exposure in Q3 follows the scale and sensitivity of the data. Manchester Airports Group said the UK Information Commissioner's Office was assessing its incident. The reported Aeromexico dataset prompted a government investigation in Mexico. BE Travel issued POPIA notifications in South Africa. Starts Publishing reported the OZmall incident to Japan's Personal Information Protection Commission.[9,21]

The first questions in any regulatory review will be basic ones: when the organisation became aware, what data was affected, which customers were in scope and when the supplier or operator notified them. These dates and records determine both the legal timetable and the credibility of the organisation's later account.

8.2 Sector Regulatory Tracker

Jurisdiction / regulator	Incident	Q3 position	Practitioner implication
United Kingdom - ICO	Manchester Airports Group	ICO assessing the incident	Preserve decision records, data mapping and notification chronology.
Mexico - government authorities	Aeromexico	Investigation opened into advertised customer dataset	Treat unverified data-sale claims as evidence to investigate, not as confirmed breach facts.
South Africa - POPIA / sector authorities	BE Travel; ATNS	Notifications / investigation reported	Coordinate privacy and operational reporting where services and personal data may both be affected.
Japan - PPC	OZmall / Starts Publishing	Incident reported to the PPC	Supplier platforms require fast affected-customer identification and notification support.

8.3 Cyber Insurance

Three insurance questions follow directly from the Q3 incidents. Does the policy cover data extortion when no systems are encrypted? Does a supplier-platform failure trigger response or business-interruption cover? And how does the wording treat an exposed key or token where no malware was used? These questions are better answered at renewal than during an incident.

9. Threat Outlook

The outlook below is based on the patterns in Q3. It is an assessment of what organisations should prepare for, not a prediction that a named attack will occur.

9.1 Ransomware and Data Extortion

Confidence level: High. Ransomware and data extortion will remain the main public threat across these sectors. The model works even when encryption fails because stolen data can still be used to demand payment or create publication pressure.

9.2 Identity and Credential Exploitation

Confidence level: High. Exposed API keys, legitimate external access and large identity repositories will continue to give attackers routes to valuable data without requiring a conventional malware intrusion.

9.3 Third Party and Supply Chain Risk

Confidence level: High. Booking, ticketing, point-of-sale and verification providers offer a wider return than a single operator. A failure at one supplier can reach many organisations at the same time.

9.4 Social Engineering Targeting Sector Staff

Confidence level: Moderate. Q3 contains less direct evidence of social engineering against sector staff than Q2. The pretexts remain available, however, because reservations, loyalty accounts, suppliers and customer-service workflows all depend on staff responding quickly to apparently legitimate requests.

9.5 Web Skimming and Customer-Facing Malware

Confidence level: Moderate. The AI-driven skimming campaign shows that malicious code on a customer-facing website can steal payment data without a conventional endpoint compromise. The technique is established; what is new is the reported use of automated agents to scale it.

9.6 Regulatory and Litigation Pressure

Confidence level: Moderate. The scale of the Manchester Airports Group, IDScan.net and Times Car incidents, together with the investigated aviation datasets, makes further regulatory scrutiny and civil claims likely. Most Q3 disclosures are still too recent for the litigation position to be clear.

9.7 Operational Technology and Physical Systems

Confidence level: Low to moderate. The ATNS investigation and the disruption at Hit and Keio show that operational environments remain exposed, but most Q3 incidents were data-extortion cases rather than attacks on physical or safety-critical systems.

9.8 Insider Threats

Confidence level: Low. The Q3 evidence contains no confirmed case of paid insider recruitment in the sectors covered here. The risk has not disappeared, but this edition does not provide enough evidence to rate it more strongly.

9.9 Monetisation and Dark Web Activity

Confidence level: High. Leak sites, publication and resale will remain closely tied to extortion. Q3 also shows why the number of listings will continue to exceed the number of independently confirmed breaches.

Assessment Summary

The strongest Q4 planning assumption is that criminals will continue to steal data first and use availability as a secondary source of pressure. Most organisations will therefore face a data and communications problem. A smaller number will face the harder operational problem of keeping reservations, reception, payments or aviation services running at the same time.

10. Recommendations

10.1 Secret and API Key Governance

Remove API keys, tokens and credentials from public web code and client-side applications.

Scan repositories, deployment packages and public websites automatically for exposed secrets.

Give each key only the permissions it needs, and rotate it immediately if exposure is suspected.

Record an owner and expiry date for every production secret.

10.2 Ransomware and Data-Extortion Readiness

Keep an extortion response plan that works even when systems are still available.

Decide in advance who validates a leak-site claim, who may communicate with the threat actor and who approves public statements.

Keep offline or isolated backups for the systems that support reception, reservations, payments and communications.

Exercise the decision to refuse a ransom, including the possibility that stolen data will be published.

10.3 Supplier, Booking and Platform Assurance

Require suppliers to notify the organisation quickly when booking or customer data may be affected.

Put access to forensic findings, affected-record lists and notification support into the contract.

Map which supplier holds each class of guest, passenger or loyalty data and where it is hosted.

Test how the organisation will warn customers when the supplier cannot yet confirm the full scope.

10.4 Customer-Facing Web, Payment and Wi-Fi Monitoring

Monitor changes to payment pages, third-party scripts and booking widgets.

Use content-security controls and integrity monitoring for externally loaded scripts.

Publish the exact names of legitimate guest and passenger Wi-Fi networks and look for close copies.

Give front-line staff one clear route for reporting an unusual website, QR code or Wi-Fi network.

10.5 Aviation Operational Resilience

Keep airport and airline commercial systems separate from safety-critical and operational environments wherever possible.

Define manual fallbacks for customer processing, communications and service recovery.

Include airport, airline, handler, caterer and technology-provider dependencies in resilience exercises.

Bring operational disruption and passenger communications into the cyber response plan.

10.6 Data Minimisation and Segmentation

Keep passports, driving licences and other identity documents only for as long as there is a clear business or legal need.

Separate identity, loyalty, payment and booking data so that one compromise does not reveal the whole customer profile.

Limit supplier access to the records needed for the service being delivered.

Review old archives and exports. Large legacy datasets remain useful to criminals even when the business has stopped using them.

10.7 Tabletop Exercise Scenarios for Hotel, Restaurant, Tourism and Aviation Environments

Scenario 1. Exposed API key and extortion. A web developer discovers that a production API key has been visible in public website code for several months. Logs show unusual access to customer records and a criminal group demands payment before publishing the data. The exercise tests how quickly the key can be revoked, how the affected records are identified, when the regulator is notified and how the organisation handles a decision not to pay.

Scenario 2. Supplier booking-platform breach. A booking supplier says guest records may have been exposed but cannot yet identify the affected properties or customers. Guests begin contacting the hotel after receiving convincing payment messages. The exercise tests supplier escalation, guest warnings, data mapping and the decision on notification before the supplier has completed its investigation.

Scenario 3. Reception and reservation outage. Ransomware takes down hotel communications and reservation processes during a high-occupancy period. The exercise tests manual check-in, room allocation, guest communications, restoration priorities and coordination with the technology provider.

Scenario 4. Rogue guest Wi-Fi. Guests report a wireless network whose name differs by one word from the official hotel or airline network. A customer says that they entered credentials into the captive portal. The exercise tests front-line recognition, technical containment, evidence collection and communication with affected customers.

Scenario 5. Unverified leak-site claim. The organisation appears on a ransomware leak site with no data sample and no evidence in internal logs. Media enquiries arrive within hours. The exercise tests whether the team can separate claim from evidence, decide whether any notification duty has been triggered and communicate before the investigation is complete.

Run each scenario with defined roles, a time limit of no more than two hours and a structured debrief that produces a written action list with owners and deadlines. Repeat the exercises at least once a year and update them as the threat picture changes.

Endnotes

The numbered endnotes below support the source markers used in the report. Appendix A is compiled from the Q3 research note and the underlying source set. Where an incident had not been independently confirmed at the research cut-off, that status is retained.

1. **BlackFog,** The State of Ransomware, July 2026. https://www.blackfog.com/the-state-of-ransomware-july-2026/
2. **BlackFog,** The State of Ransomware, August 2026. https://www.blackfog.com/the-state-of-ransomware-august-2026/
3. **Check Point Research,** July 2026 Cyber Threat Landscape. https://blog.checkpoint.com/security/july-2026-cyber-threats-surge-ransomware-attacks-double-year-over-year-as-genai-data-exposure-widens
4. **Check Point Research,** August 2026 Cyber Threat Landscape. https://blog.checkpoint.com/security/august-2026-cyber-threat-landscape-genai-data-exposure-emerges-as-a-new-enterprise-risk-as-attacks-phishing-and-ransomware-accelerate
5. **ransomware.live,** Full 2026 victim dataset export. https://data.ransomware.live/2026-victims.json
6. **Have I Been Pwned,** Manchester Airports Group breach record. https://haveibeenpwned.com/Breach/ManchesterAirportsGroup
7. **BleepingComputer,** FulcrumSec claims Manchester Airports hack, theft of 86 GB of data. https://www.bleepingcomputer.com/news/security/fulcrumsec-claims-manchester-airports-hack-theft-of-86-gb-of-data/
8. **Scott Helme,** No hacking required: the MAG data breach. https://scotthelme.co.uk/no-hacking-required-manchester-airports-group-data-breach/
9. **Manchester Airport,** Data security incident page. https://www.manchesterairport.co.uk/help/data-security-incident/
10. **The Record,** Slovenian casinos reopen after cyberattack. https://therecord.media/slovenia-cyberattack-casinos-reopen
11. **BleepingComputer,** Malicious AI agents steal 600,000 credit cards. https://www.bleepingcomputer.com/news/security/malicious-ai-agents-steal-600k-credit-cards-infect-100-plus-sites-with-skimmers/
12. **Help Net Security,** IDScan confirms breach. https://www.helpnetsecurity.com/2026/09/11/idscan-net-data-breach-153-million-drivers-licenses/
13. **Las Vegas Sun,** Delta and FAA probe rogue Wi-Fi network. https://lasvegassun.com/news/2026/aug/12/delta-faa-probe-rogue-wi-fi-network-on-las-vegas-t/
14. **Daily Maverick,** Hungry Lion listed by MedusaLocker. https://www.dailymaverick.co.za/article/2026-08-27-hungry-lion-latest-victim-in-concerning-rise-of-cyberattacks/
15. **SecNews,** Mikel Coffee claim by The Gentlemen. https://www.secnews.gr/en/726267/mikel-coffee-ransomware-the-gentlemen-claim/
16. **Morningstar / Alliance News,** accesso Technology reports IT security incident. https://www.morningstar.com/news/alliance-news/178577130536870780 0/accesso-technology-reports-it-security-incident-but-trading-in-line
17. **BleepingComputer,** 220 million traveller records exposed in APIS leak. https://www.bleepingcomputer.com/news/security/220-million-traveler-records-exposed-in-vietnam-linked-apis-leak/
18. **Born City,** Cyber incident at Atlantic hotel group. https://borncity.com/blog/en/2026/09/19/cybervorfall-bei-atlantic-hotel-gruppe-18-9-2026/

19. **BleepingComputer,** Times Car confirms data breach affecting 6.6 million user accounts. https://www.bleepingcomputer.com/news/security/times-car-confirms-data-breach-affecting-66-million-user-accounts/

20. **BleepingComputer,** Keio confirms ransomware attack disrupted business systems. https://www.bleepingcomputer.com/news/security/japans-keio-confirms-ransomware-attack-disrupted-business-systems/

21. **UPI,** Mexico opens probe into Aeromexico data breach. https://www.upi.com/Top_News/World-News/2026/09/21/latam-mexico-aeromexico-date-breach-investigation/7411790010504/

22. **CBS Atlanta,** Chick-fil-A warns customers after cyberattack exposed loyalty accounts. https://www.cbsnews.com/atlanta/news/chick-fil-a-warns-customers-in-10-states-after-cyberattack-exposed-some-loyalty-accounts/

23. **Dark Reading,** South Africa probes cyberattack on air traffic control organisation. https://www.darkreading.com/cyberattacks-data-breaches/south-africa-help-cyberattack-air-traffic-control

24. **SecurityWeek,** Cl0p names over 40 victims of PTC Windchill campaign. https://www.securityweek.com/cl0p-ransomware-group-names-over-40-victims-of-ptc-windchill-campaign/

25. **Privacy Guides,** Data Breach Roundup, 4 to 10 September 2026. https://www.privacyguides.org/news/2026/09/11/data-breach-roundup-sep-4-10-2026/

26. **Privacy Guides,** Data Breach Roundup, 25 September to 1 October 2026. https://www.privacyguides.org/news/2026/10/02/data-breach-roundup-sep-25-oct-1-2026/

27. **Claim Depot,** Corporate Travel Service data breach notification. https://www.claimdepot.com/data-breach/corporate-travel-service-2026

28. **CM Alliance,** Major cyber attacks and data breaches, September 2026. https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-data-breaches-ransomware-attacks-september-2026

29. **Igor's Lab,** Leakwatch CW 40/2026. https://igorslab.de/en/leakwatch-cw-40-2026-ai-agents-attack-vector-identity-records-zero-days

30. **Scrutex,** Ransomware attacks this week, 14 to 20 September 2026. https://scrutex.ai/blogs/ransomware-attacks-this-week-221-victims-across-47-groups-september-14-to-september-20

31. **Rhein-Zeitung,** Hahn Airport cyberattack investigation. https://www.rhein-zeitung.de/rheinland-pfalz/hacker-angriff-am-hahn-so-ist-stand-der-ermittlungen_arid-4154244.html

32. **Daily Hodl,** Waterford Hotel Group data breach notification. https://dailyhodl.com/2026/10/01/connecticut-hotel-operator-data-breach-puts-ssns-financial-and-medical-records-at-risk

33. **Security Affairs,** Keio Corporation security breach coverage. https://securityaffairs.com/?p=200027

Appendix A. Full In-Scope Incident Matrix

This appendix contains all 99 in-scope Q3 incidents after the agreed exclusions, followed by 13 earlier incidents that were disclosed or claimed during the quarter. The Q3 research source does not establish the five intrusion stages used in the Q2 appendix for most cases, so this edition preserves the evidence actually available: threat actor, attack vector, impact/data, status and date. Threat-actor claims are marked as unconfirmed.

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Refinery Hotel (USA)	Hotel	Akira	Ransomware and data extortion	15 GB claimed, including employee passports, driving licences and Social Security numbers, guest information and contracts	Claimed by threat actor (unconfirmed)	1 Jul 2026
Holiday Palace Hotel (Macau)	Hotel	APT73	Data extortion	Guest information, internal documents, photos and video claimed	Claimed by threat actor (unconfirmed)	2 Jul 2026
KT Restaurant (TH)	Restaurant and Food Service	Majinahanashi	Data extortion	1,853 files listed; leak listed 16 Aug	Claimed by threat actor (unconfirmed)	Early Jul 2026 (estimated)
Air Creebec (CA)	Aviation	Chaos	Ransomware and data extortion	Regional airline listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	6 Jul 2026
Casta Diva Group (IT)	Tourism and Travel	PayoutsKing	Data extortion	Event production group listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	6 Jul 2026
Metropolitan Entertainment and Convention Authority, Omaha (USA)	Tourism and Travel	Dark Project	Data theft and extortion	More than 500 GB claimed, including customer data, financial documents and employee data; about 100,000 files posted	Claimed by threat actor (unconfirmed)	7 Jul 2026
Sure Travel Company (HK)	Tourism and Travel	Orova	Data extortion	Travel company listed on leak site 4 Aug	Claimed by threat actor (unconfirmed)	7 Jul 2026
Red Planet Hotels (PH)	Hotel	Qilin	Ransomware and data extortion	Listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	10 Jul 2026
SH Hoteles (ES)	Hotel	DeadLock	Ransomware and data extortion	Hotel chain in Valencia and Alicante listed;	Claimed by threat actor (unconfirmed)	10 Jul 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
				download link posted		
ACU, Automobile Club of Uruguay (UY)	Tourism and Travel	DeadLock	Data extortion	Motorist and travel services club listed; download link posted to SwissTransfer	Claimed by threat actor (unconfirmed)	10 Jul 2026
BE Travel (ZA)	Tourism and Travel	Arcus Media	Ransomware	Travel voucher and administration system for a government agency; personal information may have been accessed or encrypted; POPIA notifications issued	Confirmed by victim	13 Jul 2026
URH Hoteliers (ES)	Hotel	Qilin	Ransomware and data extortion	Listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	13 Jul 2026
POWDR ski resorts (USA)	Tourism and Travel	Settra	Data extortion	Mountain resort operator listed 11 Aug; data categories not disclosed	Claimed by threat actor (unconfirmed)	13 Jul 2026
Panasonic Avionics (JP/USA)	Aviation	Coinbase Cartel	Data extortion	In-flight entertainment and connectivity supplier listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	15 Jul 2026
Sinai Grand Casino (EG)	Tourism and Travel	DragonForce	Ransomware and data extortion	Tourist casino in Sharm El Sheikh listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	16 Jul 2026
Giraudi Group, Beefbar (MC)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Owner of more than 35 restaurants listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	16 Jul 2026
Kee Wah Bakery (HK)	Restaurant and Food Service	DragonForce	Ransomware and data extortion	Bakery chain listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	16 Jul 2026
Emirates Flight Catering (AE)	Aviation	Everest	Data extortion	Airline caterer at Dubai International Airport listed 5	Claimed by threat actor (unconfirmed)	17 Jul 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
				Aug; data categories not disclosed		
Don Tortaco Mexican Grill (USA)	Restaurant and Food Service	Qilin	Ransomware and data extortion	Listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	19 Jul 2026
Tèrra Aventura (FR)	Tourism and Travel	Nova	Data extortion	Regional tourism treasure hunt app listed; proofs withheld pending contact	Claimed by threat actor (unconfirmed)	21 Jul 2026
Halona Plaza, Zuni Shopping Center (USA)	Hotel	BlackNevas	Data extortion	Operator of a supermarket, restaurant and eight room inn listed	Claimed by threat actor (unconfirmed)	22 Jul 2026
Restaurant Depot (USA)	Restaurant and Food Service	Play	Ransomware and data extortion	Food service wholesaler listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	23 Jul 2026
Record Go car rental (ES)	Tourism and Travel	Play	Ransomware and data extortion	Car rental company listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	23 Jul 2026
Sunway Berhad (MY)	Hotel	Qilin	Ransomware and data extortion	Conglomerate with hotels and theme parks listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	23 Jul 2026
Katathani Phuket Beach Resort (TH)	Hotel	DragonForce	Ransomware and data extortion	Listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	27 Jul 2026
Qube Aviation Catering (USA)	Aviation	CRPxO	Data extortion	Airline caterer listed; 22.5 GB claimed	Claimed by threat actor (unconfirmed)	27 Jul 2026
accesso Technology Group (UK)	Sector technology	Coinbase Cartel	Unauthorised access and data theft	Ticketing and queuing software for attractions; limited systems accessed, no downtime; group claims internal files	Confirmed by victim	Late Jul 2026 (claim 28 Jul)
Angel Hotel, Pershore (UK)	Hotel	The Gentlemen	Ransomware and data extortion	Hotel and restaurant listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	29 Jul 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Weilhotel (MY)	Hotel	Gunra	Ransomware and data extortion	Listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	29 Jul 2026
THY, Turkish Airlines (TR)	Aviation	CRPxO	Data extortion	Flag carrier listed; 4.2 GB claimed	Claimed by threat actor (unconfirmed)	31 Jul 2026
Nichirei (JP)	Restaurant and Food Service	RansomHouse	Unauthorised access and data extortion	Cold storage and logistics failure disrupted frozen food supply to about 5,000 partners including KFC Japan and Kura Sushi; employee and partner data later published	Confirmed by victim	13 Jul 2026
AI driven skimming campaign, unnamed Fortune 500 hospitality company and major US airline (USA)	Aviation	Unattributed, Chinese speaking operator (Gambit)	Web skimming by autonomous AI agents	At least 119 sites carried card skimmers; more than 600,000 card records stolen from two firms; campaign active July to at least 22 September	Under investigation	Jul to Sep 2026
TUI China (CN)	Tourism and Travel	DragonForce	Ransomware and data extortion	Passports, visas, internal, legal and financial documents claimed	Claimed by threat actor (unconfirmed)	3 Aug 2026
BestPriceTravel (AU)	Tourism and Travel	2019	Data theft and sale	Customer names, emails, flight and booking details, payment, refund and cancellation data offered for sale	Claimed by threat actor (unconfirmed)	4 Aug 2026
Woodhaven Lakes (USA)	Tourism and Travel	Play (claim)	Ransomware and data theft	Private recreational resort; phones, payments and facilities disrupted; local files encrypted, off-site backups intact; property owner database reportedly not breached	Confirmed by victim	6 Aug 2026
Toast (USA)	Sector technology	Cl0p	Data theft through PTC Windchill flaw	Restaurant POS provider named; 215 GB of project, backup	Claimed by threat actor (unconfirmed)	Aug 2026 (listed 12 Aug)

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
			(CVE-2026-12569)	database and log data claimed		
Club One Casino (USA)	Tourism and Travel	ThreeAM, then PEAR	Ransomware and data extortion	Card room with 24 hour restaurant claimed by two groups within two weeks	Claimed by threat actor (unconfirmed)	6 and 18 Aug 2026
Mikel Coffee (GR)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Chain of 410 stores in 19 countries; customer contact and password data claimed; no sample released	Claimed by threat actor (unconfirmed)	9 Aug 2026
Delta Air Lines Flight 591 (USA)	Aviation	Unattributed passenger	Rogue Wi-Fi access point	Fake network called Delta WiFi Fast broadcast in flight; crew disabled onboard Wi-Fi for about 30 minutes; FBI aware	Confirmed by victim	10 Aug 2026
The Minor Food Group (TH)	Restaurant and Food Service	Panzer	Data extortion	Minor International food arm with more than 2,600 outlets listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	10 Aug 2026
D and J Beverage Service (USA)	Restaurant and Food Service	Qilin	Ransomware and data extortion	Beverage distributor listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	13 Aug 2026
Zara Investment Holding (JO)	Hotel	Payload	Ransomware and data extortion	Owner of about 30 per cent of Jordan five star hotel capacity listed	Claimed by threat actor (unconfirmed)	13 Aug 2026
KFC Kosova (XK)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Regional franchise listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	14 Aug 2026
The Coffee Bean and Tea Leaf Malaysia (MY)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Café chain with more than 150 stores listed	Claimed by threat actor (unconfirmed)	14 Aug 2026
Gravity Coffee (USA)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Coffee chain listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	14 Aug 2026
Spoonful of Comfort (USA)	Restaurant and Food Service	Qilin	Ransomware and data extortion	Food gift delivery firm listed; data	Claimed by threat actor (unconfirmed)	16 Aug 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
				categories not disclosed		
Berghotel Oberhof (DE)	Hotel	ZaWoo	Ransomware and data extortion	Wellness hotel listed 30 Aug; data categories not disclosed	Claimed by threat actor (unconfirmed)	18 Aug 2026
Mihuru (DE)	Tourism and Travel	Xpl0itrs	Data extortion	Consumer travel financing firm listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	19 Aug 2026
The Margo Hotel (UK)	Hotel	Majinahanashi	Data extortion	8,080 files scheduled for publication	Claimed by threat actor (unconfirmed)	20 Aug 2026
Grand Ion Delemen Hotel (TR)	Hotel	Majinahanashi	Data extortion	5,045 files scheduled for publication	Claimed by threat actor (unconfirmed)	20 Aug 2026
Magdalena Grand Beach and Golf Resort (TT)	Hotel	The Gentlemen	Ransomware and data extortion	Tobago resort listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	21 Aug 2026
The Revel Collective (USA)	Tourism and Travel	Direwolf	Ransomware and data extortion	Listed with hospitality sector tag; data categories not disclosed	Claimed by threat actor (unconfirmed)	21 Aug 2026
Furnished Quarters (USA)	Hotel	Dark Project	Data theft and extortion	155 GB and about 198,000 files claimed, including customer, banking and financial data	Claimed by threat actor (unconfirmed)	24 Aug 2026
Hit d.d. (SI)	Tourism and Travel	Akira (claim 23 Sep)	Ransomware	Six casinos closed for about three days; hotel reception, cash registers and loyalty system disrupted; 367 GB claimed including employee IDs and client data	Confirmed by victim	Overnight 24 to 25 Aug 2026 (Akira claim 23 Sep)
Park de Rochie (NL)	Tourism and Travel	Chaos	Data extortion	Holiday park named in pre-publication countdown post	Claimed by threat actor (unconfirmed)	25 Aug 2026
Manchester Airports Group (UK)	Aviation	FulcrumSec	API key exposed in website code, data theft and extortion	About 8.7 million customer records from Manchester, Stansted and East Midlands,	Confirmed by victim	Aug 2026 (disclosed 25 to 27 Aug)

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
				revised to about 8.8 million by Have I Been Pwned; emails, phone numbers, vehicle registrations, postcodes, parking, lounge and Fast Track bookings; 86 GB claimed; data published 2 to 3 Sep after ransom refusal; ICO assessing		
Hungry Lion (ZA)	Restaurant and Food Service	MedusaLocker	Ransomware and data extortion	Point of sale data from Unity, GAAP and CoSoft systems posted; USD 50,000 demand; no customer personal data seen in samples	Claimed by threat actor (unconfirmed)	27 Aug 2026
Seabrook Island (USA)	Tourism and Travel	Akira	Ransomware and data extortion	Resort community; 55 GB claimed including employee IDs, Social Security numbers and client data	Claimed by threat actor (unconfirmed)	27 Aug 2026
Servicios Aéreos Estrella (MX)	Aviation	The Gentlemen	Ransomware and data extortion	Business aviation handler and charter operator at Toluca listed	Claimed by threat actor (unconfirmed)	28 Aug 2026
South Pacific Hotel (HK)	Hotel	Orova	Data extortion	293 room hotel listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	29 Aug 2026
First Call Hospitality (BR)	Hotel	Settra	Data extortion	Hotel management company listed 17 Sep	Claimed by threat actor (unconfirmed)	31 Aug 2026
IDScan.net (USA)	Sector technology	Unattributed, sold through Nexus marketplace	Cloud data theft over about a year	More than 153 million US and Canadian driving licence scans offered; used by bars, venues and car rental counters; FBI investigating	Confirmed by victim	Discovered 1 Sep 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Royal Plaza on Scotts (SG)	Hotel	Eclipse	Data extortion	Five star Orchard Road hotel listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	2 Sep 2026
Star Aviation (USA)	Aviation	Storm	Ransomware and data extortion	Aerospace wire harness MRO listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	2 Sep 2026
McDonald's Ecuador (EC)	Restaurant and Food Service	Vexy	Ransomware and data extortion	Arcos Dorados franchise listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	3 Sep 2026
Toronto Pearson, GTAA (CA)	Aviation	Unattributed	Social media account hijack	Airport X account briefly hijacked for crypto promotion; operations and security systems unaffected	Confirmed by victim	4 Sep 2026
The Big Table Group (UK)	Restaurant and Food Service	Qilin	Ransomware and data extortion	Operator of Bella Italia, Café Rouge and Las Iguanas listed	Claimed by threat actor (unconfirmed)	5 Sep 2026
Líder Aviação (BR)	Aviation	The Gentlemen	Ransomware and data extortion	Latin America's largest business aviation operator listed	Claimed by threat actor (unconfirmed)	5 Sep 2026
AbacoViaggi (IT)	Tourism and Travel	The Gentlemen	Data extortion	Bologna travel agency; customer data, financials, correspondence and credentials claimed	Claimed by threat actor (unconfirmed)	7 Sep 2026
Lake Beverage (USA)	Restaurant and Food Service	Settra	Data extortion	Beer distributor listed; about 165 GB claimed	Claimed by threat actor (unconfirmed)	7 Sep 2026
TTG Asia Media (SG)	Tourism and Travel	Eclipse	Data extortion	Travel trade publisher listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	8 Sep 2026
Air Canada (CA)	Aviation	The Gentlemen	Data extortion	Flag carrier listed; 51,409 files claimed; airline has not confirmed	Claimed by threat actor (unconfirmed)	9 Sep 2026
Moscone Center, ASM Global (USA)	Tourism and Travel	Settra	Data extortion	San Francisco convention centre operator listed with narrative post	Claimed by threat actor (unconfirmed)	11 Sep 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Egyptian Airports Company (EG)	Aviation	Krybit	Ransomware and data extortion	State airport operator listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	12 Sep 2026
Tiflis Palace (GE)	Hotel	Krybit	Ransomware and data extortion	Boutique hotel in Tbilisi listed	Claimed by threat actor (unconfirmed)	12 Sep 2026
La Sultana Hotels (MA)	Hotel	Krybit	Ransomware and data extortion	Moroccan boutique hotel group listed	Claimed by threat actor (unconfirmed)	12 Sep 2026
Praveg Caves Jawai (IN)	Hotel	MedusaLocker	Ransomware	Safari resort; listing names its hotel management and point of sale software and staff	Claimed by threat actor (unconfirmed)	12 Sep 2026
Dang Invest Group (CZ)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Operator of more than 70 Asian fast food outlets in three countries listed	Claimed by threat actor (unconfirmed)	14 Sep 2026
Iveta (HR)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Bakery and café chain supplying Dalmatian hotels and restaurants listed	Claimed by threat actor (unconfirmed)	14 Sep 2026
Atlas Ocean Voyages (USA)	Tourism and Travel	Booba Project	Data extortion	Expedition cruise line listed; 37 GB claimed	Claimed by threat actor (unconfirmed)	14 Sep 2026
Gelarti (PE)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Ice cream parlour chain with 39 shops listed	Claimed by threat actor (unconfirmed)	14 Sep 2026
EVA Airways (TW)	Aviation	Unattributed	Unauthorised network access	Internal network infiltrated via suspicious IPs; employee names and business contacts accessed; operations unaffected; disclosed through TWSE	Confirmed by victim	15 Sep 2026
Evergreen Aviation Technologies (TW)	Aviation	Unattributed	Cyberattack on internal systems	Maintenance provider; endpoints isolated, core operations normal; data impact undisclosed	Confirmed by victim	15 Sep 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Gran Hotel Inglés (ES)	Hotel	Qilin	Ransomware and data extortion	Listed on leak site; data categories not disclosed	Claimed by threat actor (unconfirmed)	17 Sep 2026
Ligue-se Grupo (PT)	Sector technology	The Gentlemen	Ransomware and data extortion	Madeira IT group supplying hotel technology listed	Claimed by threat actor (unconfirmed)	24 Sep 2026
Atlantic Hotels Group (DE)	Hotel	Unattributed	Website compromise (ClickFix)	Atlantic, SEVERIN*S and unique by ATLANTIC hotel websites served a fake Cloudflare check that pushed PowerShell malware to visitors; sites offline until 21 Sep; company says no guest or company data stolen	Confirmed by victim	18 Sep 2026
Roan Luxury Camping Holidays (NL)	Tourism and Travel	INC Ransom	Data extortion	Luxury camping tour operator listed	Claimed by threat actor (unconfirmed)	18 Sep 2026
Aeroméxico (MX)	Aviation	Unattributed, advertised on Telegram	Data theft, origin unclear	Database of 1.1 GB with more than 15 million customer records advertised, sample including public officials; ministry probe opened; airline found no card or password evidence; possibly recycled October 2025 data	Under investigation	18 Sep 2026
Touring Club Suisse (CH)	Tourism and Travel	Qilin	Ransomware and data extortion	Listed; data categories not disclosed	Claimed by threat actor (unconfirmed)	20 Sep 2026
Maritim Hotels via Amadeus iHotelier (DE)	Hotel	Unattributed	Third-party reservation platform breach	8,716 guests notified; stays 1 Aug 2026 to 30 Sep 2027; postal addresses, emails and phone numbers; no payment or passport data	Confirmed by victim	Disclosed 18 to 23 Sep 2026
Air Tanzania (TZ)	Aviation	Krybit	Ransomware and data extortion	Flag carrier listed; data	Claimed by threat actor (unconfirmed)	24 Sep 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
				categories not disclosed		
Jones the Grocer (AU)	Restaurant and Food Service	Krybit	Ransomware and data extortion	Gourmet food retail and café chain listed	Claimed by threat actor (unconfirmed)	24 Sep 2026
Times Mobility, Times Car (JP)	Tourism and Travel	Unattributed	Unauthorised access to web systems	About 6.6 million current and former car sharing and rental accounts plus corporate accounts, including 1.6 million identity verification records such as driving licence images; access from early Sep, theft confirmed 28 Sep; card data not affected; reported to PPC and police; Park24 group company	Confirmed by victim	Detected 25 Sep 2026
Keio Group, Keio Plaza Hotel (JP)	Hotel	Unattributed	Ransomware	Group networks partly shut down; hotel communications and reservation processes disrupted; trains ran normally; customer data exposure under investigation	Confirmed by victim	26 Sep 2026
Air Traffic and Navigation Services (ZA)	Aviation	Unattributed	Ransomware, possible insider involvement	Operational technology for weather related air traffic services hit; possible exfiltration to IP addresses in China; forensic tender issued	Under investigation	Not stated (disclosed 26 Sep 2026)
Starts Publishing, OZmall (JP)	Sector technology	Unattributed	Unauthorised access from overseas	Restaurant, hotel and salon booking platform; up to 442,779 email addresses, some with names and prefecture; no cards or passwords; reported to PPC 28 Sep	Confirmed by victim	Discovered 26 Sep 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Holiday Inn Vilnius (LT)	Hotel	SafePay	Ransomware and data theft	IHG-branded hotel listed 28 Sep; data of more than 500 guests and 100 employees reported stolen; publicly disclosed 2 Oct	Claimed by threat actor (unconfirmed)	28 Sep 2026
Solaria (ID)	Restaurant and Food Service	The Gentlemen	Ransomware and data extortion	Restaurant chain with more than 200 outlets listed	Claimed by threat actor (unconfirmed)	29 Sep 2026
Camp Ozark, Ozark Interests (USA)	Tourism and Travel	Unattributed	Data breach	Names, addresses, bank and payment card data; Texas attorney general filing	Disclosed via breach notification	29 Sep 2026

Earlier attacks disclosed or claimed during Q3 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Corporate Travel Service (USA)	Tourism and Travel	Unattributed	Network intrusion	Travel agency and tour operator; Social Security numbers and medical records among data; about 2,900 notified in four states	Disclosed via breach notification	3 to 11 Dec 2025
Bee Cheng Hiang (SG)	Restaurant and Food Service	None, accidental	AI-generated bulk email without BCC	95,364 customer email addresses exposed; Singapore's first AI-related breach; PDPC undertaking published 21 Sep, public 30 Sep	Confirmed by victim	Apr 2026
Frontier Airlines (USA)	Aviation	Scattered Lapsus$ Hunters (reported)	Data theft from storage account	Employee and customer Social Security numbers, addresses and ID numbers; notifications from 9 Jul; two class actions filed 15 Jul; ExfilSquad separately listed Frontier on 26 Jul claiming about 2.4 million records with personal and flight data, its relationship to the	Disclosed via breach notification	12 May and 3 Jun 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
				May intrusion unconfirmed		
Vietnam linked APIS database (VN)	Aviation	Unattributed	Misconfigured database exposure	220 million passenger and crew records from 2017 to 2026 with passport and flight data; open until 8 June; disclosed 8 Sep	Under investigation	Found 3 Jun 2026
Hotel de la Bourse, Mulhouse (FR)	Hotel	LockBit 5	Ransomware	Listed 11 Jul; data categories not disclosed	Claimed by threat actor (unconfirmed)	10 Jun 2026
JS Hotels (ES)	Hotel	LockBit 5	Ransomware	Operator of ten Majorca hotels listed 11 Jul	Claimed by threat actor (unconfirmed)	15 Jun 2026
Chick-fil-A (USA)	Restaurant and Food Service	Unattributed	Credential stuffing	Chick-fil-A One loyalty accounts; names, emails, QR codes, last four card digits and gift balances; more than 71,000 accounts per New York notification; disclosed 20 to 22 Jul	Disclosed via breach notification	17 to 19 Jun 2026
Stadttheater Gießen (DE)	Tourism and Travel	The Gentlemen	Ransomware	All data and backups made inaccessible; performances continued; listed 1 Jul	Confirmed by victim	18 Jun 2026
Plitvice Lakes National Park (HR)	Tourism and Travel	Qilin	Ransomware	Ticketing and electronic payments disrupted, cash only at some outlets; listed 25 Jul	Confirmed by victim	24 Jun 2026
Hahn Airport (DE)	Aviation	SafePay	Ransomware and data extortion	Flights unaffected; exfiltrated data published on leak site; prosecutors investigating sabotage and attempted extortion	Confirmed by victim	Jun 2026 (claim 6 Jul)
Furama Bukit Bintang (MY)	Hotel	NightSpire	Data extortion	Executive, HR and IT data claimed; listed 27 Jul	Claimed by threat actor (unconfirmed)	27 Jun 2026

Organisation	Sector	Threat Actor	Attack Vector	Impact / Data	Status	Date
Arkın Group hotels and casino (CY)	Hotel	BlackNevas	Data theft and sale	About 1.4 TB claimed, including guest passports, payment data and casino player records; listed 30 Jun and 4 Aug	Claimed by threat actor (unconfirmed)	30 Jun 2026
Waterford Hotel Group and LMD Holding (USA)	Hotel	Interlock (claimed 11 May)	Unauthorised network access	Names, driving licence, Social Security, passport, taxpayer, financial, payment card, credential, medical and health insurance data may be affected; notifications reported 1 Oct	Disclosed via breach notification	Identified 5 May 2026

Appendix B. Detailed Threat Actor Profiles

The Gentlemen

Q3 in-scope activity: 16 incidents. Preferred pattern: Ransomware and data extortion; high-volume leak-site listing. Sector evidence: Restaurant and food service, aviation, hotel and sector-technology targets. Assessed risk to the covered sectors: Critical.

Named Q3 targets in the in-scope dataset: Giraudi Group, Beefbar (MC); Angel Hotel, Pershore (UK); Mikel Coffee (GR); KFC Kosova (XK); The Coffee Bean and Tea Leaf Malaysia (MY); Gravity Coffee (USA); Magdalena Grand Beach and Golf Resort (TT); Servicios Aéreos Estrella (MX); Líder Aviação (BR); AbacoViaggi (IT); Air Canada (CA); Dang Invest Group (CZ); Iveta (HR); Gelarti (PE); Ligue-se Grupo (PT); Solaria (ID).

Qilin

Q3 in-scope activity: 9 incidents. Preferred pattern: Ransomware and data extortion; repeated sector listings. Sector evidence: Hotels, restaurants and tourism businesses. Assessed risk to the covered sectors: Critical.

Named Q3 targets in the in-scope dataset: Red Planet Hotels (PH); URH Hoteliers (ES); Don Tortaco Mexican Grill (USA); Sunway Berhad (MY); D and J Beverage Service (USA); Spoonful of Comfort (USA); The Big Table Group (UK); Gran Hotel Inglés (ES); Touring Club Suisse (CH).

Krybit

Q3 in-scope activity: 5 incidents. Preferred pattern: Ransomware and data extortion. Sector evidence: Multiple hotel and aviation claims. Assessed risk to the covered sectors: High.

Named Q3 targets in the in-scope dataset: Egyptian Airports Company (EG); Tiflis Palace (GE); La Sultana Hotels (MA); Air Tanzania (TZ); Jones the Grocer (AU).

Settra

Q3 in-scope activity: 4 incidents. Preferred pattern: Data extortion. Sector evidence: Tourism and hotel claims. Assessed risk to the covered sectors: High.

Named Q3 targets in the in-scope dataset: POWDR ski resorts (USA); First Call Hospitality (BR); Lake Beverage (USA); Moscone Center, ASM Global (USA).

DragonForce

Q3 in-scope activity: 4 incidents. Preferred pattern: Ransomware and data extortion. Sector evidence: Tourism, hotels and restaurants. Assessed risk to the covered sectors: High.

Named Q3 targets in the in-scope dataset: Sinai Grand Casino (EG); Kee Wah Bakery (HK); Katathani Phuket Beach Resort (TH); TUI China (CN).

Akira

Q3 in-scope activity: 3 incidents. Preferred pattern: Ransomware and data extortion. Sector evidence: Refinery Hotel and Hit; major operational disruption at Hit. Assessed risk to the covered sectors: High.

Named Q3 targets in the in-scope dataset: Refinery Hotel (USA); Hit d.d. (SI); Seabrook Island (USA).

FulcrumSec

Q3 in-scope activity: 1 incident. Preferred pattern: Data theft and extortion linked to an exposed API key. Sector evidence: Manchester Airports Group. Assessed risk to the covered sectors: Critical.

Named Q3 targets in the in-scope dataset: Manchester Airports Group (UK).

Contact

Prof Alexandros Paraskevas (PhD)
Director of the International Centre for Hospitality and Aviation Resilience Management (ICHARM)
Professor in Strategic Risk Management
Chair of Hospitality Management and Doctoral Programmes Lead
London Geller College of Hospitality and Tourism
University of West London | St. Mary's Road, Ealing, London W5 5RF, United Kingdom

Direct Line +44 (0)20 8231 2279
Mobile +44 (0)779 382 2593
E-mail Alexandros.Paraskevas@uwl.ac.uk
Website uwl.ac.uk/users/alexandros-paraskevas

ICHARM

The International Centre for Hospitality and Aviation Resilience Management (ICHARM) at the University of West London focuses on risk, resilience, and performance in hotels, restaurants, and tourism organisations. The team brings together hospitality, cyber security, and legal expertise to support boards and senior managers in service based businesses.

The ICHARM Cyber Threat Intelligence team tracks attack patterns, threat actors, and legal outcomes that affect hotels, restaurant and food service operators, tourism brands, and their technology providers. It uses regulatory filings, incident reports, dark web and open source monitoring, and sector specific threat feeds to build an evidence base for decision making in hospitality and tourism.

© 2026 International Centre for Hospitality and Aviation Resilience Management, University of West London. This report is provided for general information and situational awareness only. It does not constitute legal, financial, or professional advice, and should not be relied upon as the sole basis for any decision. Incident data is drawn from regulatory filings, public disclosures, and open and closed source intelligence, and should be verified before operational use.