Cyberint
A Check Point Company

TRAVEL & TOUR OPERATIONS INDUSTRY THREAT LANDSCAPE

By Josh Puentes, Manasa Pisipati and Ben Johnathan Neeman

May 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyberint, now a Check Point Company conducted a threat landscape report focusing on the Travel and Tour Operation Industry. The following report outlines recent cyber events, cyber threat predictions, and an overview of Cyberint services as a solution to mitigating digital threats.

From 2023 to 2025, the global travel sector faced a surge in targeted cyber attacks, including DDoS disruptions, ransomware incidents, data breaches via misconfigured cloud storage, and third-party supply chain compromises. The report includes an outline of events spanning worldwide. It also includes a list of the prominent TTPs (tools and techniques) relating to the attackers and a list of related IOCs that should be noted and blocked.

Below are the trend predictions Cyberint, now a Check Point Company anticipates, based on the related incidents:

DDoS Attacks Disrupting Booking Systems

These attacks are often timed to peak travel periods and exploit the industry's reliance on real-time online services. Threat actor groups are expected to continue leveraging botnets to cripple operations, potentially leading to extortion demands for service restoration.

Data Breaches via Misconfigured Cloud Storage

Attackers are increasingly using advanced tools and automated scripts to identify and exfiltrate data from exposed cloud storage. Small to mid-sized travel companies without strong DevSecOps practices remain highly vulnerable.

Phishing and Credential Exploitation

Attackers are using advanced social engineering techniques, including impersonation and AI-generated phishing lures, to harvest employee credentials. These attacks enable ransomware deployment, internal data exfiltration, and system persistence.

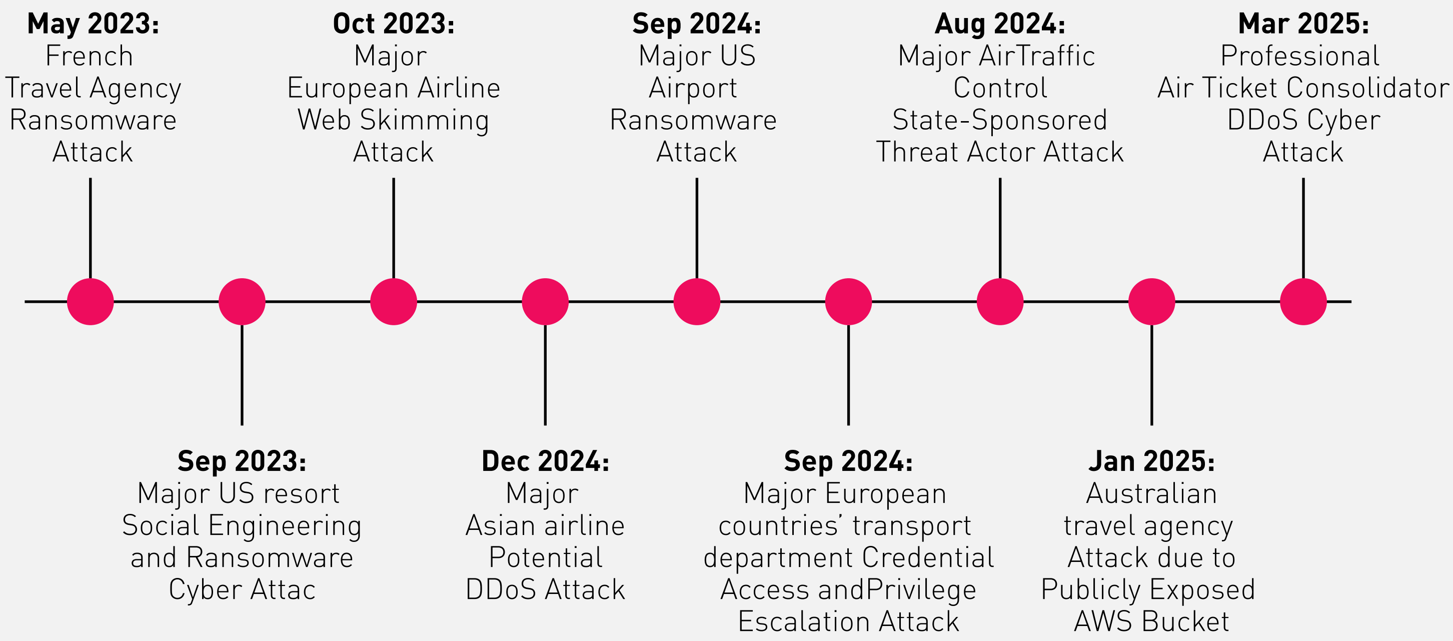
Supply Chain Compromise and Third-Party Risks

Threat actors are bypassing hardened perimeters by targeting vendors in payment processing, authentication, and cloud infrastructure, often leveraging outdated or insecure applications to infiltrate core systems and exfiltrate sensitive data.

To mitigate these evolving threats, Cyberint, now a Check Point Company provides continuous Threat Intelligence (TI) and Attack Surface Monitoring (ASM) tailored to the travel sector external risk environment. We detect early indicators of compromise, exposed assets, and threat actor activity through comprehensive monitoring across an extensive pool of sources. This proactive intelligence approach enables travel organizations to stay ahead of targeted threats and minimize operational and reputational impact.

CYBER INCIDENTS

TIMELINE OF NOTABLE EVENTS



May 2023:
French
Travel Agency
Ransomware
Attack

Sep 2023:
Major US resort
Social Engineering
and Ransomware
Cyber Attac

Oct 2023:
Major
European Airline
Web Skimming
Attack

Dec 2024:
Major
Asian airline
Potential
DDoS Attack

Sep 2024:
Major US
Airport
Ransomware
Attack

Sep 2024:
Major European
countries' transport
department Credential
Access andPrivilege
Escalation Attack

Aug 2024:
Major AirTraffic
Control
State-Sponsored
Threat Actor Attack

Jan 2025:
Australian
travel agency
Attack due to
Publicly Exposed
AWS Bucket

Mar 2025:
Professional
Air Ticket Consolidator
DDoS Cyber
Attack

Figure 1: Timeline of Cyber Attacks Covered in this Report

CYBER INCIDENTS DETAILS

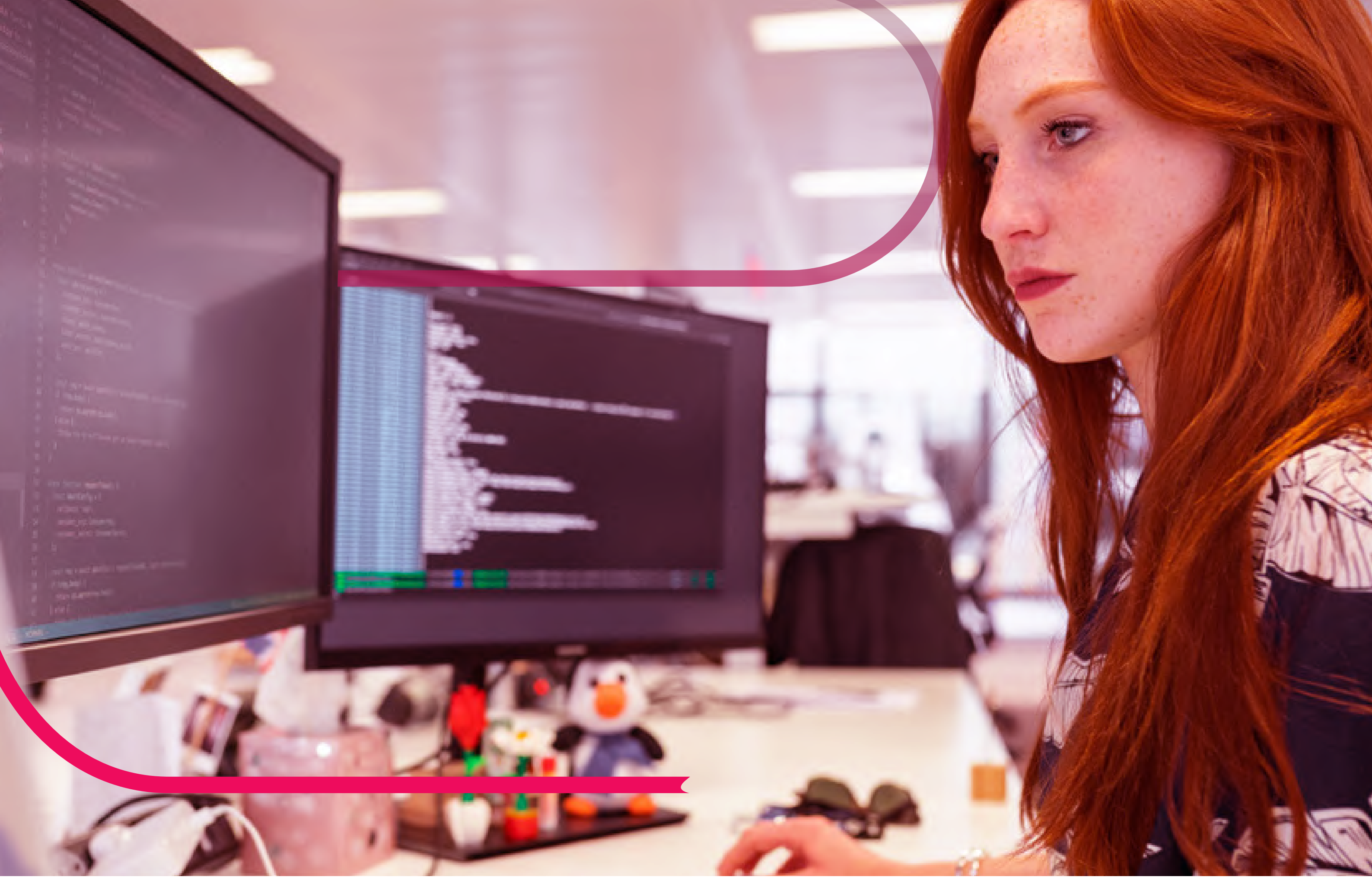
A professional air ticket consolidator DDoS Attack

In March 2025, a cyber attack disrupted a professional air ticket consolidator's operations, impacting its customers in Germany, Austria, Switzerland, and worldwide. Their booking system was impacted due to a potential "DDOS" attack.

Autralian Travel agency attack due to publicly exposed AWS bucket

In January 2025, the Australian travel agency was attacked, which led to the breach of 112,000 records from the company's non-password-protected database with a size of 26.8GB, including details such as passport images, travel visas, travel itineraries and tickets, and partial credit card numbers of customers. Spreadsheets containing detailed information of more than 13,000 customers, which included their names, email addresses, trip costs, and destinations, were discovered to have been leaked. While most impacted travelers are Australians, customers from New Zealand, Ireland, and Britain have also been affected.

The breach was due to a publicly exposed Amazon AWS Cloud Storage bucket that was incorrectly configured. These attacks usually begin with searching for exposed systems or misconfigured cloud storage. Tools or scripts were used to scan for open S3 buckets or cloud storage services (e.g., Bucket Finder, S3Scanner, Shodan, Censys, or Grayhat Warfare). Threat actors also leverage keyword-based automations to look for files like passwords.txt, .env, db_backup.sql, etc.



A major Air Traffic Control State-Sponsored Threat Actor Attack

In August 2024, the German Air Traffic Control's administrative IT infrastructure, which handles internal office communications, was attacked. This allowed unauthorized access to sensitive data. Fancy Bear (aka APT28), a threat actor attributed to Russia's military intelligence service, was attributed to this attack.

A major European countries' transport department Credential Access and Privilege Escalation Attack

In September 2024, Transport for London was hit with a cyber attack, which caused them to temporarily suspend applications for access cards due to concerns over system security.

This also affected the ability to register new cards, issue refunds for incomplete pay-as-you-go journeys made using contactless cards, and improve the booking system for the Dial-a-Ride service. Also, the live travel data feed was impacted. While pre-existing bookings were honored, new bookings could only be made by phone until the system was restored. Data on 5,000 people was accessed, including names, contact details, and Oyster card refund data. This included bank account numbers and sort codes.

Attackers reportedly used LicensingUI.exe (a signed Windows binary) to execute payloads. TfL had to reset 30,000 employee passwords in person, indicating the scale of the breach. The threat actor may have established persistence and elevated privileges, possibly using scheduled tasks or admin tokens.

Major US Airport Ransomware Attack

In September 2024, several critical systems at A major US Airport were affected due to a cyber attack attributed to Rhysida affiliates.

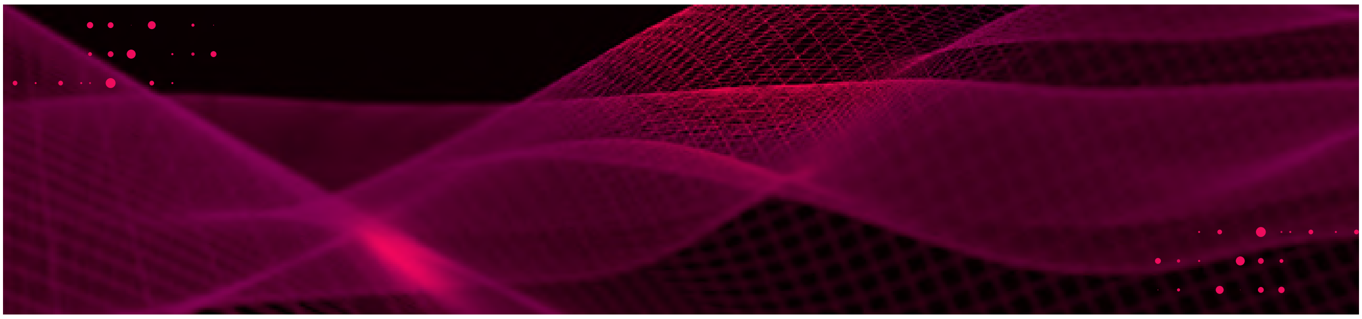
Delays in luggage processing led to bags being delivered to travelers well after arrival. Due to system outages, passengers had to use handwritten boarding passes. Internal port systems were encrypted, hindering the restoration process.

The threat actors accessed and downloaded some personal information from previously used Port systems for employee, contractor, and parking data (90000 individuals). The downloaded information included names, dates of birth, Social Security numbers (or the last four digits of Social Security numbers), driver's license or other government identification card numbers, and medical information.

Rhysida actors operate in a Ransomware-as-a-service (RaaS) capacity, where ransomware tools and infrastructure are leased out in a profit-sharing model. Rhysida actors have been observed leveraging external-facing remote services to access and persist within a network initially. They have also been observed authenticating to internal VPN access points with compromised valid credentials, notably because organizations lack MFA enabled by default. Additionally, they have been observed exploiting Zerologon - a critical elevation of privileges vulnerability in Microsoft's Netlogon Remote Protocol- and conducting successful phishing attempts.

Major Asian Airline Potential DDoS Attack

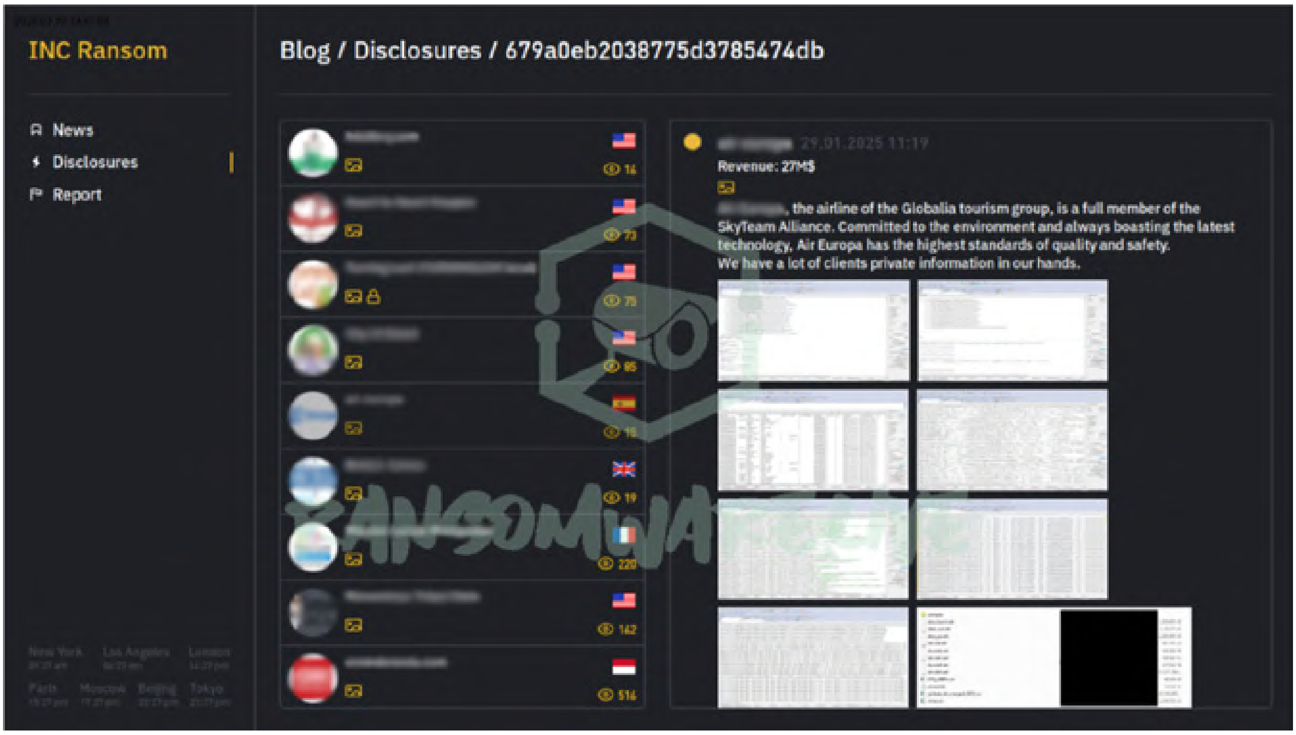
In December 2024, a major Asian airline was the victim of a cyber attack that caused flight delays. While the airline did not publicly identify the specific threat actor, it confirmed that no customer data was leaked or computer viruses were detected. The incident involved a surge in traffic, suggesting a DDoS attack, which disrupted the airline's systems and ticket sales.



A Major European Airline Web Skimming Attack

In October 2023, IncRansom (A Russian Hacking Group) gained unauthorized access to the airline's payment system. While the method of the attack has not been confirmed, it is most likely through web skimming.

The breach exposed sensitive customer data, including credit card information such as card numbers, expiration dates, and CVV codes. The airline promptly notified affected customers and advised them to cancel their cards to prevent potential fraudulent use. In March 2024, the airline updated its disclosure, revealing that additional personal information, such as names, ID or passport numbers, dates of birth, phone numbers, email addresses, and nationalities, had been exposed.



Blog / Disclosures / 679a0eb2038775d3785474db

[redacted] 29.01.2025 11:19

Revenue: 27M$

[redacted], the airline of the Globalia tourism group, is a full member of the SkyTeam Alliance. Committed to the environment and always boasting the latest technology, Air Europa has the highest standards of quality and safety.
We have a lot of clients private information in our hands.

Figure 2: Screenshot from INCRansomware DLS affecting European Airline

A major resort Social Engineering and Ransomware Cyber Attack

In September 2023, A major US resort chain was affected by a cyber attack, a combined effort of Scattered Spider and ALPHV.

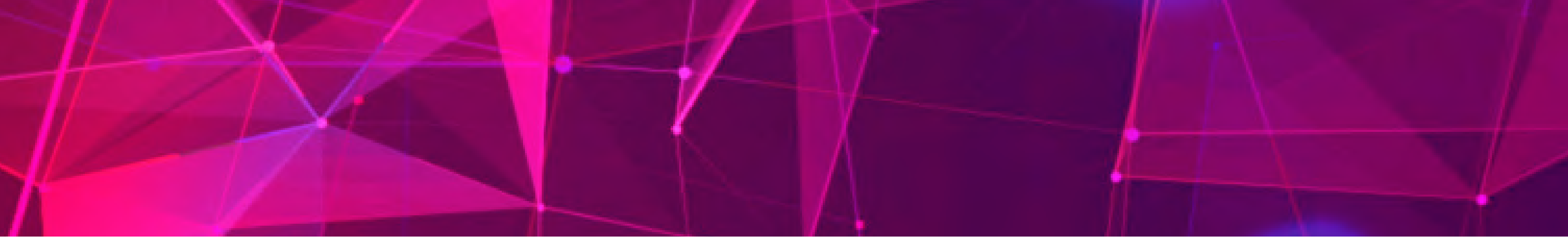
Scattered Spider members researched the company's employees on LinkedIn to gather information. They impersonated an employee and convinced the IT help desk to provide login credentials. With these, the attackers gained administrator access to the resort's Okta and Azure environments, allowing them to move laterally within the systems. ALPHV then deployed ransomware across several VMware ESXi hypervisor servers.

These servers hosted thousands of virtual machines that supported critical hospitality systems such as gaming machines, online reservation systems, digital room keys, and websites. ALPHV also claims to have exfiltrated 6 TB of customer information during this time, upon which they initiated negotiations with the resort to prevent the public release of the stolen data.

French travel agency Ransomware Attack

In May 2023, Lockbit attacked a French travel agency. Following the agency's refusal to pay the ransom, LockBit published approximately 7,000 to 10,000 passport photocopies on the dark web. These documents were collected from clients participating in group travel, constituting about 2% of the agency's customer base. Lockbit works through a RaaS (Ransomware as a Service) model. Please refer to the appendix for their TTPs.

(For further information about TTPs and IOCs based on individual threat actors, please refer to the Appendix).



TOP 10 MOST CRITICAL TTPS IN THIS SECTOR

The TTPs below have been listed as severe based on their impact, frequency in real-world incidents, and difficulty to detect or mitigate.

T1078	**Valid Accounts** Used for persistence and evasion by almost all major actors
T1190	**Exploit Public-Facing Application** Common initial access point (e.g., Citrix, VPN flaws)
T1059	**Command and Scripting Interprete** Core execution method (Bash, PowerShell, etc.)
T1566	**Phishing** Widely used by both ransomware and APT actors for initial access
T1027	**Obfuscated Files or Information** Key defense evasion technique used to avoid detection
T1055	**Process Injection** Critical for evading AV/EDR and escalating privileges
T1003.003	**LSASS Memory Dumping** Credential harvesting, crucial for lateral movement
T1021.001	**Remote Desktop Protocol (RDP)** Popular for lateral movement and post-exploitation
T1112	**Modify Registry** Used to disable protections, establish persistence
T1486	**Data Encrypted for Impact** Core ransomware activity-file encryption and extortion

Figure 3: List of Top 10 TTPs associated with Tour Operations and Travel Sector

TREND PREDICTIONS

The following predictions are derived from analyzing recent cyber incidents targeting the travel sector and travel business operations, including DDoS attacks, misconfigured cloud storage, social engineering, and ransomware.

Each prediction focuses on specific attack vectors observed in incidents between 2023–2025, projecting how these threats could evolve and impact travel businesses and operations in the future.

1 SURGE IN DDOS ATTACKS TARGETING BOOKING AND TICKETING SYSTEMS

The **Major attacks in march 2025 and December 2024** highlight critical attacks that involved **DDoS campaigns** that disrupted crucial booking and ticketing systems, causing operational delays and customer dissatisfaction. These attacks exploited the travel industry's reliance on real-time online platforms/systems.

In the future, threat actors will likely **continue deploying DDoS attacks** to overwhelm booking systems or airline ticketing platforms with the aim of **disrupting peak travel seasons** (e.g., holidays). In addition to rising geopolitical tensions, nation-state-sponsored cyber attacks will likely also become more frequent and sophisticated with the aim to disrupt critical infrastructure and financial systems aimed at destabilizing economies.

Attackers will likely leverage botnets enhanced by **AI-driven** traffic amplification to bypass traditional DDoS defenses. In aviation, around 1/4 of incidents stem from vendor vulnerabilities, offering threat actors avenues to amplify traffic surges using AI-driven botnets. Smaller travel agencies with limited cyber security budgets could be particularly vulnerable, facing downtime and revenue losses.

If this trend continues, there could be a rise in extortion schemes where attackers demand ransoms to halt DDoS campaigns, exploiting the sector's need for uninterrupted service. This tactic was seen in another sector with a 2024 healthcare ransomware attack, where BlackCat/ALPHV demanded millions to restore critical systems, highlighting the profitability of targeting time-sensitive operations. This ultimately would demand a need for the sector to invest in cloud-based DDoS protection, audit vendor security, and stress-test booking platforms.

2 INCREASED DATA BREACHES VIA MISCONFIGURED CLOUD STORAGE

In 2025, an Australian travel company experienced a significant data breach when a cloud storage bucket on **AWS was left publicly accessible** without a password. As a result, over 112,000 customer records were exposed—including scanned passports and partial credit card numbers. This incident illustrates a major vulnerability affecting the broader travel and tourism industry: misconfigured cloud storage systems.

Threat actors are increasingly automating the discovery and exploitation of misconfigured cloud storage—particularly on platforms like AWS and Azure. Tools such as Bucket Finder, S3Scanner, and search engines like Shodan and Censys allow attackers to easily locate publicly accessible buckets. Once identified, overly permissive permissions (e.g., READ, LIST, or WRITE) are exploited to anonymously access or alter stored data. Attackers then deploy keyword-based scripts using AWS CLI or boto3 to hunt for sensitive files such as .env, passwords.txt, or db_backup.sql. If HTTPS is not enforced, the data can even be exfiltrated over unencrypted channels.

As the travel and tourism industry continues its shift to cloud infrastructure, particularly among small to mid-sized operators lacking robust cyber security controls, misconfigured cloud storage will remain one of the most exploited vulnerabilities. The use of automated scanning tools and AI-driven search tactics will only accelerate, allowing attackers to identify and extract valuable data at scale. We can expect an increase in targeted extortion and data-leak-based fraud, pushing regulatory bodies to tighten compliance standards and forcing businesses to implement continuous configuration audits, strict access controls, and end-to-end encryption policies.

3 PHISHING CAMPAIGNS EXPLOITING EMPLOYEE CREDENTIALS

The 2023 attack on a major US resort revealed a rising threat pattern: phishing and impersonation attacks are being used as the entry point to compromise internal systems. Threat actor Scattered Spider successfully posed as an employee after researching LinkedIn profiles, convincing IT help desk staff to hand over credentials, and deploying ransomware that crippled operational systems.

In 2025, we can expect a surge in **AI-powered phishing campaigns** specifically targeting frontline and support staff at travel agencies, airlines, and airport operators. This is especially critical with over 70% of attacks in the aviation sector focused on stealing login details and unauthorized IT infrastructure access. Attackers will use AI-generated emails mimicking trusted vendors or executives, as seen in The above's case, to trick staff into providing access to systems like reservation platforms or payment gateways.

The travel sector's high employee turnover and remote work trends will increase vulnerabilities. Potential increases in double-extortion tactics, where stolen customer data (e.g., passports, credit cards) are leaked if ransoms are unpaid could evolve.

Phishing attacks have long been a favored tactic among cyber criminals and with the integration of generative AI, these attacks are poised to become significantly more sophisticated. Attackers will leverage AI to craft highly personalized phishing emails, texts, or social media messages, tailored to individual targets by analyzing publicly available data. Additionally, sophisticated phishing websites are increasingly being supplemented with AI-powered chatbots. These chatbots mimic support personnel with human-like language, similar typing speeds, and dynamic content generation, making it challenging to discern their authenticity.

Newer AI speech models also enable highly convincing speech imitation. This capability provides criminals with further social engineering opportunities through phishing calls, where they can impersonate support staff, bankers, and other authoritative figures to gain access to private information or systems. Moreover, these AI tools also provide non-English-speaking Threat Actors an opportunity to target U.S personnel with higher chances of success.

4 SUPPLY CHAIN ATTACKS VIA THIRD-PARTY VENDORS

The breach of a major European Airline in 2024 likely involved web skimming through a compromised payment system, exposing credit card details and personal information. Similarly, **2024 US airport attack** underscored third-party system vulnerabilities, with Rhysida affiliates gaining access to employee and contractor data. These incidents reflect a broader trend: the exploitation of public-facing applications **(T1190)** and supply chain weaknesses that expose high-value systems in the travel sector.

With the growing dependence on cloud services and multi-vendor ecosystems, attackers are likely to continue exploiting the weakest links in digital supply chains. In 2025, **supply chain attacks** targeting third-party vendors, such as payment processors, booking platforms, and identity verification services, could escalate. Adversaries may focus on infiltrating smaller, less secure vendors as entry points to compromise larger travel organizations. Once inside, attackers often capture input data **(T1056)**, extract sensitive customer or financial information from internal systems and repositories **(T1213)**, and exfiltrate it via trusted web services or cloud platforms **(T1048.003)**, which helps them evade traditional security detection.

These attacks have the potential to result in large-scale data exfiltration, financial fraud, and operational disruption, especially for companies relying on outdated vendor software, which increases exposure to zero-day vulnerabilities. Threat actors are also expected to continue opportunistically targeting organizations with weak supply chain defenses, capitalizing on businesses' lack of control over their third-party partners.

The European Network and Information Security Agency (ENISA) has flagged supply chain risks as a growing concern, highlighting their stealthy nature, complexity, and wide-reaching consequences. Many organizations across sectors remain underprepared for these threats. The travel industry is particularly vulnerable due to its heavy reliance on cloud platforms and intricate vendor ecosystems.

Additionally, more organizations are adopting AI large-language models (LLMs) at increasing rates during 2024, and more are expected to join throughout 2025. Threat Actors are aware of this new trend and are seeking to exploit it by carrying out data poisoning attacks on training models that LLMs are based on.

CYBERINT, NOW A CHECK POINT COMPANY SOLUTIONS

Given the recent emerging threat trends, it's essential to understand the range of services Cyberint offers to help safeguard against these risks.

Cyberint, now a Check Point Company monitors various assets, including domains, emails, external IP addresses, high-impact employees, and more. Each asset is carefully configured to meet crucial needs as security teams maneuver the many challenges they face throughout the year.

These assets are monitored daily in the Cyberint solution through attack surface monitoring (ASM) automation, threat intelligence gathering, phishing detection, and dedicated analyst collaboration.

ATTACK SURFACE MONITORING

The Attack Surface Monitoring module in the Cyberint solution performs non-intrusive, daily, and weekly scans on the following categories of assets:

- **Domains**
- **Subdomains**
- **IP Addresses**
- **Azure Data Lake / Storage Blobs**
- **Google Cloud Storage**
- **Amazon S3 Buckets**

Automated daily exposure scans continuously monitor vulnerable technologies, misconfigurations, exploitable or open ports, and other potential exposure items. When an issue is detected, an alert is automatically generated and sent to the alerts module, where the team can review and determine the appropriate next steps.

This daily scan is imperative for monitoring potential vulnerabilities on external-facing assets, especially Amazon S3 buckets, as it directly relates to the aforementioned ticketing system Cyber Attack, in which threat actors accessed an incorrectly configured cloud storage bucket.

The Attack Surface Monitoring (ASM) module provides continuous visibility into a wide range of digital assets through non-intrusive daily and weekly scans. It identifies vulnerabilities, misconfigurations, and exposed services across domains, IPs, and cloud storage, while leveraging public data and optional cloud integrations to uncover associated assets that may not be directly provided.

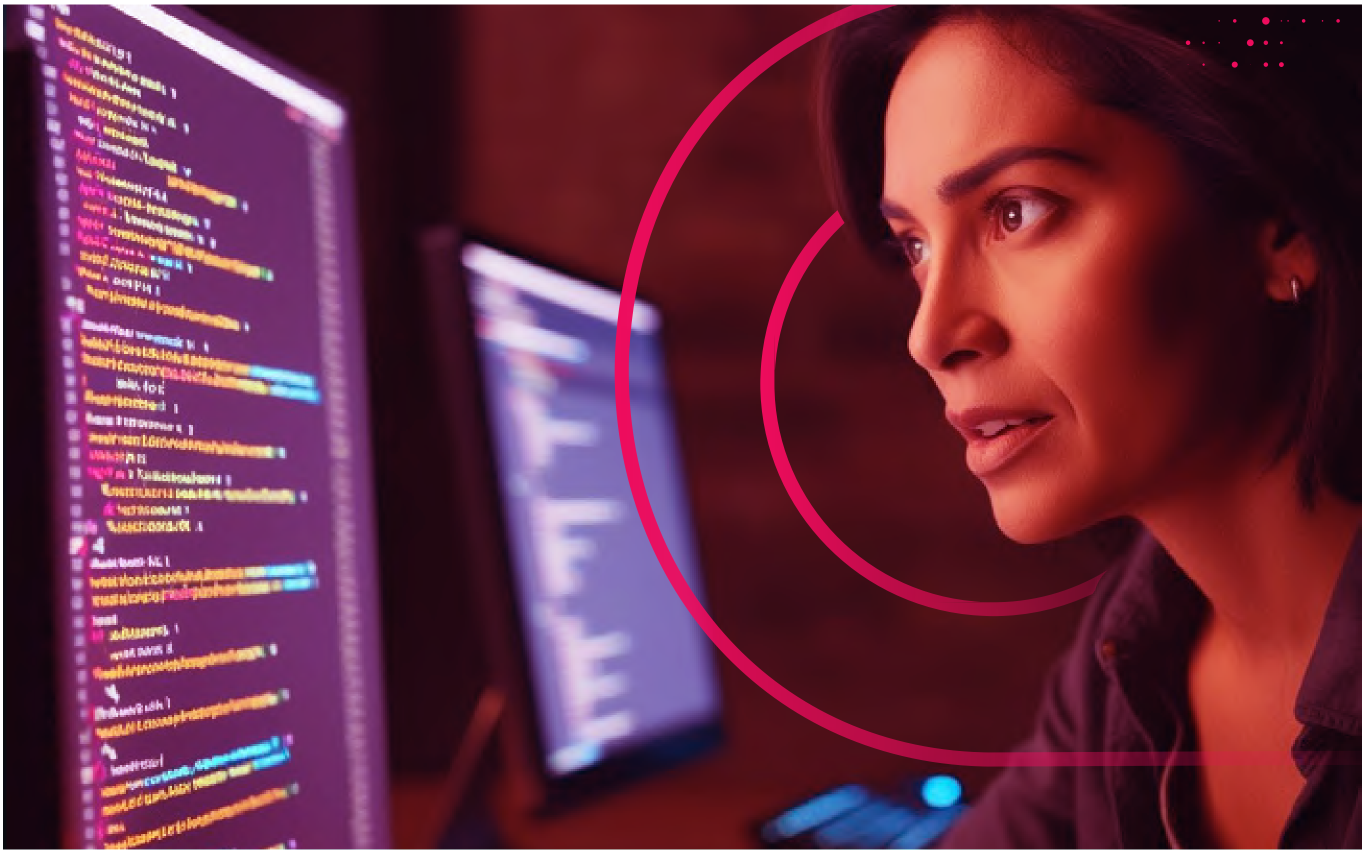
This comprehensive approach ensures organizations maintain awareness of their external exposure and can take timely action on any issues detected.

THREAT INTELLIGENCE MONITORING

Phishing Detection

Under Cyberint's phishing protection, core domain assets can be flagged for both Threat Intelligence and Attack Surface Monitoring, enabling automatic detection of suspicious lookalike domains.

To supplement the automation, Cyberint, now a Check Point Company's Phishing Beacon proactively identifies phishing sites by embedding a nonintrusive script within the protected website. It alerts us when malicious actors attempt to clone that same site on unauthorized domains.



Threat Hunting

Threat intelligence monitoring is strengthened through the strategic designation of key assets. Once identified, these assets are continuously monitored across a broad range of intelligence sources, including underground forums, code repositories, and social media, to surface potential risks. The dedicated analyst reviews collected intelligence daily and notifies relevant security teams of any relevant threats.

Additionally, the analyst team at Cyberint, now a Check Point Company constantly consume a variety of reports that allow us to adapt continuously to the ever-evolving threat landscape as it pertains to specific industries and makes recommendations on best practices to mitigate emerging threats.

Supply Chain Monitoring

Additionally, supply chain monitoring is a service Cyberint, now a Check Point Company offers that would allow for the addition of specific third-party vendors used by the customer organization to be continuously monitored and, if detected, automate alerts pertaining to:

- Supply Chain Vendor name mentions in Darknet forums
- Supply Chain Vendor name mentions in breaches
- A Vendor suffering from an ongoing ransomware attack
- Emerging phishing campaign related to the supply chain vendor
- Supply Chain Vendor Source Code Leaked
- Supply Chain Vendor Offered for Sale

Continuous monitoring of third-party vendors is essential because their systems and security practices can directly impact on the organization's risk exposure.

This monitoring remains highly relevant to both current and emerging cyber threat landscapes, as threat actors increasingly target supply chain vendors as an entry point to compromise larger organizations. By proactively identifying vulnerabilities, breaches, or suspicious activity within the vendor's ecosystem, one can quickly respond to potential threats and prevent downstream consequences to the company's environment.

The combination of broad intelligence collection and the dedicated analyst's ongoing monitoring and analysis helps provide a clearer understanding of the organization's external threat landscape.

DEDICATED ANALYST SERVICES

The analyst provides many services alongside daily threat monitoring and alerting. The dedicated analyst is considered the expert of the Cyberint Solution, looking to maximize the platform's use and ensure that all modules are running efficiently and as intended.

Some tasks the analysts perform to fine-tune the solution on an ongoing basis include:

- **Asset Configuration –** The analyst ensures that each asset received is configured to meet the customer's needs.

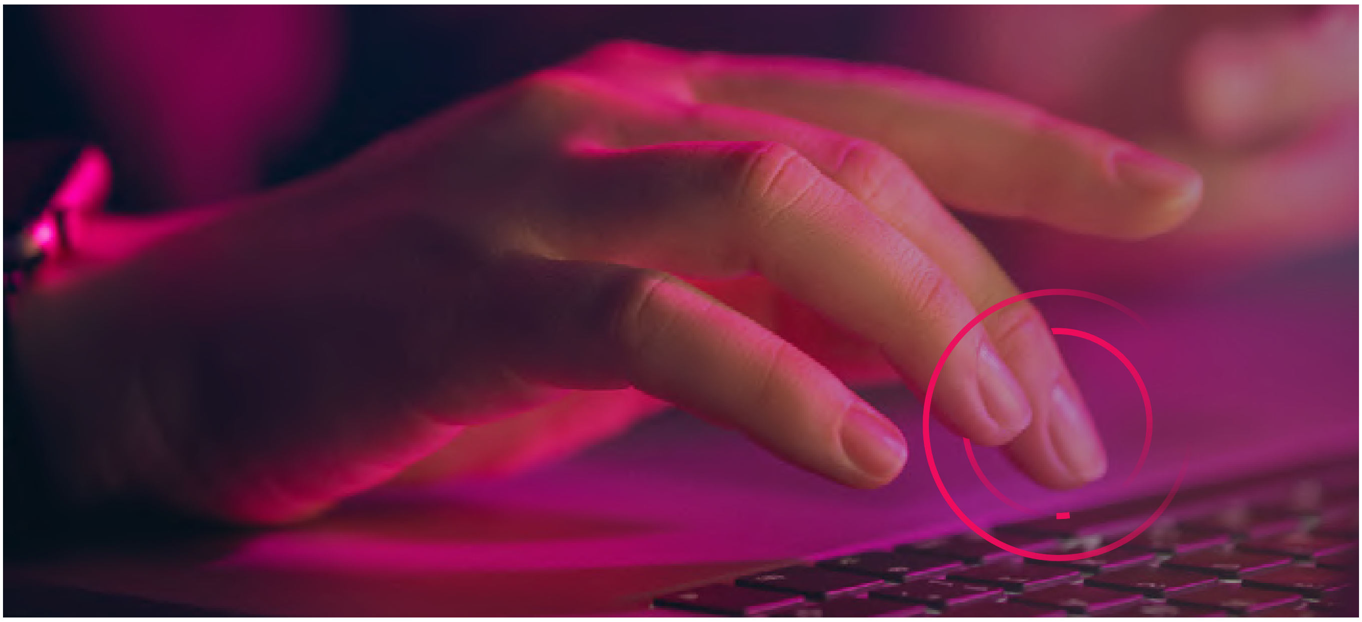
- **Asset Updating –** Incrementally, the analyst requests updates for to ensure up-to-date coverage.

- **Environment Metrics Monitoring -** Analysts monitor automation and alerts to suggest ways to tune the environment to meet customer needs.

- **Alert Configuration -** Analysts review alerting like such as closure reasons and customer feedback to make suggestions on alert configurations (i.e; disablements, severity overrides, corporate password policy tuning).

The dedicated analyst also holds regular meetings—typically monthly, to present key alerts and discussion points, providing customers with clear insight into the most impactful findings and the overall value of the analyst's ongoing efforts.

Over time, analysts see the raw intelligence gathered mentioning the customer assets daily, and become experts tailored to the intelligence requirements and strategy of the customer. With this expertise, they can make further intelligence suggestions in strategic calls such as a Priority Requirement Alignment (PIR) to ensure alignment with the company's strategic goals, or Quarterly Business Review (QBR) meetings.



CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

The travel industry is facing an evolving external threat landscape, driven by enhanced DDoS attacks, phishing campaigns, cloud misconfigurations, and supply chain compromises. As attackers adapt, so must travel organizations' defensive strategies, particularly in how they understand and respond to threats beyond their internal perimeters.

As an important external threat intelligence monitoring partner, Cyberint, now a Check Point Company is positioned to play a critical role in strengthening cyber resilience by delivering timely, relevant, and actionable insights.

By combining real-time intelligence collection, external attack surface visibility, and analyst-driven insights, Cyberint, now a Check Point Company helps anticipate and mitigate cyber threats before they impact operations. In a sector as time-sensitive and customer-facing as travel, having a partner focused on what's happening beyond the company's firewall is no longer optional, it's essential.

RECOMMENDATIONS

Based on recent cyber attacks targeting the travel industry, Cyberint, now a Check Point Company recommends the following:

1 DEFENDING AGAINST DDOS ATTACKS ON BOOKING AND TICKETING SYSTEMS

As we anticipate a rise in AI-driven DDoS attacks targeting critical travel platforms during high-traffic periods, our recommendations are as follows:

- **Use Cyberint to Monitor for pre-attack chatter** across underground forums, Telegram channels, and botnet markets where DDoS campaigns are planned or advertised.
- **Track mentions of your core platforms** and digital infrastructure to detect early warning signs of potential targeting.
- **Implement DDoS Prevention Mechanism:** enforce cloud-based DDoS protection, audit vendor security, and stress-test booking platforms.

2 PREVENTING DATA BREACHES FROM MISCONFIGURED CLOUD STORAGE

Cyberint, now a Check Point Company anticipates increasing exploitation of open cloud buckets, leading to sensitive data leaks in the sector. Thus, our recommendations are as follows:

- **Use Cyberint to Monitor for exposed data linked to your brand** or customers across breach forums, paste sites, and searchable repositories.
- **Use Cyberint to Enforce Monitoring for configuration-related leaks**, such as .env, .bak, or backup files detected in threat actor dumps or public buckets.
- **Utilize Cyberint's ASM (Attack Surface Monitoring) Detection** to continuously scan for newly exposed cloud assets, misconfigured storage, and unauthorized changes to your cloud footprint.

3 MITIGATING AI-POWERED PHISHING AND CREDENTIAL HARVESTING

Cyberint, now a Check Point Company anticipates a rise in Sophisticated phishing using generative AI and impersonation targeting frontline staff in the sector. Thus, our recommendations are as follows:

- **Enforce Monitoring for impersonation of your brand, executives, or customer support teams** across social media, domain registrations, and phishing kits. Cyberint, now a Check Point Company provides this service.

- **Enforce Early phishing infrastructure Monitoring** through lookalike domains and cloned sites using our phishing detection. Cyberint, now a Check Point Company provides this service.

4 MONITORING THIRD-PARTY RISK AND SUPPLY CHAIN EXPLOITATION

Cyberint, now a Check Point Company anticipates growing attacks through vulnerable vendors, payment platforms, and outdated third-party tools. Thus, our recommendations are as follows:

- **Continuously monitor vendor ecosystems** for compromise indicators, leaked credentials, or data mentioning your organization via third-party connections. Cyberint, now a Check Point Company offers a third party vendor monitoring solution.

- Track **sector-specific supply chain** breaches and provide contextual threat intelligence to assess if your environment is indirectly impacted.

- **Block IOCs:** To protect your internal systems, we recommend importing the provided IOC list into your endpoint protection platform and configuring it to block or quarantine any matching threats. Additionally, apply the IPs and domains to your internal DNS or host-based firewall policies to prevent communication with known malicious infrastructure. Please see the IOC list in pages 26-37.

APPENDIX

CONSOLIDATED TTP LIST

Technique ID	Technique Name
T1003.003	Security Account Manager (SAM)
T1005	Data from Local System
T1012	Query Registry
T1016	System Network Configuration Discovery
T1018	Remote System Discovery
T1021	Remote Services
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1021.004	SSH
T1027	Obfuscated Files or Information
T1033	System Owner/User Discovery
T1047	Windows Management Instrumentation
T1048.003	Exfiltration Over Alternative Protocol: SMB/Windows Admin Shares
T1055	Process Injection
T1055.002	Portable Executable Injection
T1056	Input Capture
T1056.004	Credential API Hooking
T1057	Process Discovery
T1059	Command and Scripting Interpreter
T1059.001	PowerShell
T1059.003	Windows Command Shell
T1069.001	Permission Groups Discovery: Local Groups
T1069.002	Permission Groups Discovery: Global Groups
T1070.001	Indicator Removal from Tools: File Deletion
T1070.004	Indicator Removal from Tools: File System Metadata Deletion
T1071	Application Layer Protocol
T1078	Valid Accounts
T1087.002	T1087.002

Technique ID	Technique Name
T1110	Brute Force
T1112	Modify Registry
T1190	Exploit Public-Facing Application
T1210	Exploitation for Privilege Escalation
T1213	Data from Information Repositories
T1219	Remote Access Tools
T1482	Domain Trust Discovery
T1486	Data Encrypted for Impact
T1497	Virtualization/Sandbox Evasion
T1530	Data from Cloud Storage Object
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1548	Abuse Elevation Control Mechanism
T1564.003	Hide Artifacts: Hidden Files and Directories
T1566	Phishing
T1567	Exfiltration Over Web Service
T1567.002	Exfiltration Over Web Service: Web Shell
T1580	Data from Local System
T1587	Acquire Infrastructure
T1589	Gather Victim Identity Information
T1595	Active Scanning
T1596.001	Gather Victim Host Information: System Information Discovery
T1657	Application Layer Protocol: Web Protocols

IOCS BY THREAT ACTOR

Rhysida

IOC Type	Technique Name	Hash / Email / IP	Description
C2 IP Address	5.39.222[.]67	N/A	Command and Control Server
C2 IP Address	5.255.99[.]59	N/A	Command and Control Server
C2 IP Address	51.77.102[.]106	N/A	Command and Control Server
C2 IP Address	108.62.118[.]136	N/A	Command and Control Server
C2 IP Address	108.62.141[.]161	N/A	Command and Control Server
C2 IP Address	146.70.104[.]249	N/A	Command and Control Server
C2 IP Address	156.96.62[.]58	N/A	Command and Control Server
C2 IP Address	157.154.194[.]6	N/A	Command and Control Server
Email Address	rhysidaeverywhere@onionmail[.]org	N/A	Email associated with Rhysida
Email Address	rhysidaofficial@onionmail[.]org	N/A	Email associated with Rhysida
SHA256 Hash	48f559e00c472d9ffe3965ab92c6d298f8fb3a3f0d6d203cd2069bfca4bf3a57	Sock5.sh	File used in Rhysida operations
SHA256 Hash	edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef	PsExec64.exe	File used in Rhysida operations
SHA256 Hash	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b	PsExec.exe	File used in Rhysida operations

IOC Type	Technique Name	Hash / Email / IP	Description
SHA256 Hash	201d8e77ccc2575d910d47042a986480b1da28cf0033e7ee726ad9d45ccf4daa	PsGetsid64.exe	File used in Rhysida operations
SHA256 Hash	a48ac157609888471bf8578fb8b2aef6b0068f7e0742fccf2e0e288b0b2cfdfb	PsGetsid.exe	File used in Rhysida operations
SHA256 Hash	de73b73eeb156f877de61f4a6975d06759292ed69f31aaf06c9811f3311e03e7	PsInfo64.exe	File used in Rhysida operations
SHA256 Hash	951b1b5fd5cb13cde159cebc7c60465587e2061363d1d8847ab78b6c4fba7501	PsInfo.exe	File used in Rhysida operations
SHA256 Hash	fdadb6e15c52c41a31e3c22659dd490d5b616e017d1b1aa6070008ce09ed27ea	PsLoggedon64.exe	File used in Rhysida operations
SHA256 Hash	d689cb1dbd2e4c06cd15e51a6871c406c595790ddcdcd7dc8d0401c7183720ef	PsLoggedon.exe	File used in Rhysida operations
SHA256 Hash	554f523914cdbaed8b17527170502199c185bd69a41c81102c50dbb0e5e5a78d	PsService64.exe	File used in Rhysida operations
SHA256 Hash	d3a816fe5d545a80e4639b34b90d92d1039eb71ef59e6e81b3c0e043a45b751c	PsService.exe	File used in Rhysida operations
SHA256 Hash	8329bcbadc7f81539a4969ca13f0be5b8eb7652b912324a1926fc9bfb6ec005a	Eula.txt	File used in Rhysida operations
SHA256 Hash	be922312978a53c92a49fefd2c9f9cc098767b36f0e4d2e829d24725df65bc21	psfile64.exe	File used in Rhysida operations
SHA256 Hash	4243dc8b991f5f8b3c0f233ca2110a1e03a1d716c3f51e88faf1d59b8242d329	psfile.exe	File used in Rhysida operations
SHA256 Hash	7ba47558c99e18c2c6449be804b5e765c48d3a70ceaa04c1e0fae67ff1d7178d	pskill64.exe	File used in Rhysida operations
SHA256 Hash	5ef168f83b55d2cbd2426afc5e6fa8161270fa6a2a312831332dc472c95dfa42	pskill.exe	File used in Rhysida operations
SHA256 Hash	d3247f03dcd7b9335344ebba76a0b92370f32f1cb0e480c734da52db2bd8df60	pslist64.exe	File used in Rhysida operations
SHA256 Hash	ed05f5d462767b3986583188000143f0eb24f7d89605523a28950e72e6b9039a	pslist.exe	File used in Rhysida operations

IOC Type	Technique Name	Hash / Email / IP	Description
SHA256 Hash	5e55b4caf47a248a10abd009617684e969dbe5c448d087ee8178262aaab68636	psloglist64.exe	File used in Rhysida operations
SHA256 Hash	dcdb9bd39b6014434190a9949dedf633726fdb470e95cc47cdaa47c1964b969f	psloglist.exe	File used in Rhysida operations
SHA256 Hash	8d950068f46a04e77ad6637c680cccf5d703a1828fbd6bdca513268af4f2170f	pspasswd64.exe	File used in Rhysida operations
SHA256 Hash	6ed5d50cf9d07db73eaa92c5405f6b1bf670028c602c605dfa7d4fcb80ef0801	pspasswd.exe	File used in Rhysida operations
SHA256 Hash	d1f718d219930e57794bdadf9dda61406294b0759038cef282f7544b44b92285	psping64.exe	File used in Rhysida operations
SHA256 Hash	355b4a82313074999bd8fa1332b1ed00034e63bd2a0d0367e2622f35d75cf140	psping.exe	File used in Rhysida operations
SHA256 Hash	4226738489c2a67852d51dbf96574f33e44e509bc265b950d495da79bb457400	psshutdown64.exe	File used in Rhysida operations
SHA256 Hash	13fd3ad690c73cf0ad26c6716d4e9d1581b47c22fb7518b1d3bf9cfb8f9e9123	psshutdown.exe	File used in Rhysida operations
SHA256 Hash	4bf8fbb7db583e1aacbf36c5f740d012c8321f221066cc68107031bd8b6bc1ee	pssuspend64.exe	File used in Rhysida operations
SHA256 Hash	95a922e178075fb771066db4ab1bd70c7016f794709d514ab1c7f11500f016cd	pssuspend.exe	File used in Rhysida operations
SHA256 Hash	a9ca77dfe03ce15004157727bb43ba66f00ceb215362c9b3d199f000edaa8d61	PSTools.zip	File used in Rhysida operations
SHA256 Hash	2813b6c07d17d25670163e0f66453b42d2f157bf2e42007806ebc6bb9d114acc	Pstools.chm	File used in Rhysida operations
SHA256 Hash	8e43d1ddbd5c129055528a93f1e3fab0ecdf73a8a7ba9713dc4c3e216d7e5db4	pversion.txt	File used in Rhysida operations

Lockbit

IOC Type	Indicator
C2 IP Address	185.215.229[.]44
C2 IP Address	185.215.229[.]45
C2 IP Address	185.215.229[.]46
C2 IP Address	185.215.229[.]47
C2 IP Address	185.215.229[.]48
Domain Name	lockbit[.]pro
Domain Name	lockbit[.]info
Domain Name	lockbit[.]com
Domain Name	lockbit[.]org
Email Address	lockbit@protonmail[.]com
Email Address	support@lockbit[.]pro
File Name	lockbit.exe
SHA256 Hash	23e742dc0f0ec5953993d8f2e5e4399b21353600042d1b9ef95fc9ad26811d729
File Name	lockbit-ransomware.exe
SHA256 Hash	2d96d8315e46517a6d61f93b774951af41b0621c240fd1a315c458aa77978fd99
File Name	lockbit.txt
SHA256 Hash	ccd9da93ab1c6fc3005b72c8a105ffdeeea0e7c9e5b6ec30a100907bc7fe773cf
File Name	ransom_note.txt
SHA256 Hash	292c2717ed5863497f34ad0715455191e4a567f24ff78870b517c2922dcd58e9
File Name	lockbit_6341d6e5844c8289.exe
SHA256 Hash	f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea
File Name	Salary_Lockheed_Martin_job_opportunities_confidential[.]doc
MD5 Hash	18a352d33c8c01b6a196adce176c5a96
MD5 Hash	9661c01af31a41caef2ccd3b6be06e60
MD5 Hash	3c9e550d41f3de930e678776a6e018ed
MD5 Hash	b354eaf3061b4099aecac523eb5466a3
SHA1 Hash	7e303af8c686a0c98fa87a34de1ffcf08f64a093
SHA1 Hash	e09dae6d33cffd7f6f38b62b71c484e5b12b4b79
SHA1 Hash	a118e1e110e285fb82495defe7d1c570d922ee0d

IOC Type	Indicator
SHA1 Hash	774e4e11015b6ff9f3f79aa43770c057d98fbc24
URL	hxxps://temp[.]sh/AErDa/LockBit_6341D6E5844C8289[.]exe
Registry Key	HKCU\Software\LockBit
Registry Key	HKLM\Software\LockBit
Mutex	LockBitMutex
Process Name	lockbit.exe
Process Name	lockbit-ransomware.exe
File Extension	lockbit
File Extension	lockbit_ransomware

IncRansom

Type	Indicator	Description
File Artifact	.INC	File extension used
File Artifact	INC-README.txt	Ransom note filename
File Artifact	INC-README.html	Alternate ransom note filename
Registry Artifact	C:\source\INC Encryptor\Release\INC Encryptor.pdb	Debugger path in binary
Wallpaper Change	Desktop wallpaper	Modified to display ransom note
Tool	NetScan.exe	Network scanning
Tool	Advanced IP Scanner	Network discovery
Tool	AnyDesk.exe	Remote desktop access
Tool	TightVNC	Remote desktop access

Type	Indicator	Description
Tool	.PsExec	Remote command execution
Tool	Mimikatz	Credential dumping
Tool	HackTool.Win32.ProcTerminator.A	Process termination
Tool	HackTool.PS1.VeeamCreds.A	Credential dumping from Veeam
Tool	7-Zip	Archiving data
Tool	MEGAsync	Cloud-based exfiltration
Encryption	AES	Encryption algorithm
Encryption	Fast, Medium, Slow	Modes used for data skipping/encryption
Encryption	Shadow Copy Deletion	Deletes Volume Shadow Copies
Email	gansbronz[at]gmail[.]com	Ransomware contact email
Onion URL	lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd[.]onion	Dark web leak site
SHA-256	ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49	Lynx Encryptor
SHA-256	571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b	Lynx Encryptor
SHA-256	eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc	Lynx Encryptor

Fancy Bear

IOC Type	Indicator
C2 IP Address	185.215.229[.]44
C2 IP Address	185.215.229[.]45
C2 IP Address	185.215.229[.]46
C2 IP Address	185.215.229[.]47
C2 IP Address	185.215.229[.]48
Domain Name	lockbit[.]pro
Domain Name	lockbit[.]info
Domain Name	lockbit[.]com
Domain Name	lockbit[.]org
Email Address	lockbit@protonmail[.]com
Email Address	support@lockbit[.]pro
File Name	lockbit.exe
SHA256 Hash	23e742dc0f0ec5953993d8f2e5e4399b21353600042d1b9ef95fc9ad26811d729
File Name	lockbit-ransomware.exe
SHA256 Hash	2d96d8315e46517a6d61f93b774951af41b0621c240fd1a315c458aa77978fd99
File Name	lockbit.txt
SHA256 Hash	ccd9da93ab1c6fc3005b72c8a105ffdeeea0e7c9e5b6ec30a100907bc7fe773cf
File Name	ransom_note.txt
SHA256 Hash	292c2717ed5863497f34ad0715455191e4a567f24ff78870b517c2922dcd58e9
File Name	lockbit_6341d6e5844c8289.exe
SHA256 Hash	f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea
File Name	Salary_Lockheed_Martin_job_opportunities_confidential[.]doc
MD5 Hash	18a352d33c8c01b6a196adce176c5a96
MD5 Hash	9661c01af31a41caef2ccd3b6be06e60
MD5 Hash	3c9e550d41f3de930e678776a6e018ed
MD5 Hash	b354eaf3061b4099aecac523eb5466a3
SHA1 Hash	7e303af8c686a0c98fa87a34de1ffcf08f64a093
SHA1 Hash	e09dae6d33cffd7f6f38b62b71c484e5b12b4b79
SHA1 Hash	a118e1e110e285fb82495defe7d1c570d922ee0d

IOC Type	Indicator
SHA1 Hash	774e4e11015b6ff9f3f79aa43770c057d98fbc24
URL	hxxps://temp[.]sh/AErDa/LockBit_6341D6E5844C8289[.]exe
Registry Key	HKCU\Software\LockBit
Registry Key	HKLM\Software\LockBit
Mutex	LockBitMutex
Process Name	lockbit.exe
Process Name	lockbit-ransomware.exe
File Extension	.lockbit
File Extension	.lockbit_ransomware

ALPHV

IOC Type	Value	Description	File Name (if any)
MD5	944153fb9692634d6c70899b83676575	ALPHV Windows Encryptor	703cCX9YcHMV2.exe
MD5	341d43d4d5c2e526cadd88ae8da70c1c	Anti Virus Tools Killer	File used in Rhysida operations
MD5	34aac5719824e5f13b80d6fe23cbfa07	CobaltStrike BEACON	LMtool.exe
MD5	eea9ab1f36394769d65909f6ae81834b	CobaltStrike BEACON	Info.exe / ConnectivityDiagnos.exe
MD5	379bf8c60b091974f856f08475a03b04	ALPHV Linux Encryptor	him
MD5	ebca4398e949286cb7f7f6c68c28e838	SimpleHelp Remote Management tool	first.exe
MD5	c04c386b945ccc04627d1a885b500edf	Tunneler Tool	conhost.exe
MD5	824d0e31fd08220a25c06baee1044818	Anti Virus Tools Killer	ibmModule.dll

IOC Type	Value	Description	File Name (if any)
MD5	61804a029e9b1753d58a6bf0274c25a6	MeshCentral Agent	WPEHOSTSVC64.exe
MD5	83deea3b61b6a734e7e4a566dbb6bffa	ScreenConnect & attacker tools installer	deployService.exe
MD5	8738b8637a20fa65c6e64d84d1cfe570	Suspected Proxy Tool	socks32.exe
SHA256	c64300cf8bacc4e42e74715edf3f8c3287a780c9c0a38b0d9675d01e7e231f16	ALPHV Windows Encryptor	—
SHA256	1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5	Anti Virus Tools Killer	—
SHA256	3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71	CobaltStrike BEACON	—
SHA256	af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021	CobaltStrike BEACON	—
SHA256	bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1	ALPHV Linux Encryptor	—
SHA256	5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905	SimpleHelp Remote Management tool	—
SHA256	bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e	Tunneler Tool	—
SHA256	732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0	Anti Virus Tools Killer	—
SHA1	3dd0f674526f30729bced4271e6b7eb0bb890c52	ALPHV Windows Encryptor	—
SHA1	d6d442e8b3b0aef856ac86391e4a57bcb93c19ad	Anti Virus Tools Killer	—
SHA1	6b52543e4097f7c39cc913d55c0044fcf673f6fc	CobaltStrike BEACON	—
SHA1	004ba0454feb2c4033ff0bdb2ff67388af0c41b6	CobaltStrike BEACON	—

IOC Type	Value	Description	File Name (if any)
SHA1	430bd437162d4c60227288fa6a82cde8a5f87100	SimpleHelp Remote Management tool	—
SHA1	1376ac8b5a126bb163423948bd1c7f861b4bfe32	Tunneler Tool	—
SHA1	380f941f8047904607210add4c6da2da8f8cd398	Anti Virus Tools Killer	—
Domain	resources.docusong[.]com	Command and Control Server	—
Domain	Fisa99.screenconnect[.]com	ScreenConnect Remote Access	—
Domain	pcrendal[.]com	Command and Control Server	—
Domain	instance-qqemas-relay[.]screenconnect[.]com	ScreenConnect Remote Access	—
Domain	instance-rbjvws-relay.screenconnect[.]com	ScreenConnect Remote Access	—
IP Address	5.199.168.24	Command and Control Server	—
IP Address	91.92.254.193	SimpleHelp Remote Access	—
IP Address	5.199.168[.]233	IP used by Threat Actor	—
IP Address	92.223.89[.]55	IP used by Threat Actor	—
IP Address	185.195.59[.]218	IP used by Threat Actor	—
IP Address	51.159.103[.]112	IP used by Threat Actor	—
IP Address	45.32.141[.]168	Command and Control Server	—
IP Address	45.77.0[.]92	Command and Control Server	—

Fancy Bear

Type	Indicator	Description
File Extension	.exe	Common malware payload
File Extension	.dll	Common malware payload
File Extension	.ps1	Used in PowerShell scripts for exploitation
Malware Hash	ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49	Known malware sample
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\*	Persistence
Mutex	Global\ScatteredSpiderMutex	Avoid multiple instances
Tool	AnyDesk	Remote desktop access
Tool	ScreenConnect	Remote desktop access
Tool	Mimikatz	Credential dumping
Tool	secretdump	Credential dumping
Tool	PsExec	Remote execution
Tool	7-Zip	File compression and archiving
Tool	MEGAsync	Cloud-based data exfiltration
Encryption	AES	Encryption algorithm
Email	gansbronz[at]gmail[.]com	Ransomware contact
Domain	lynxblog[.]net	Phishing or C2 domain
Domain	transfer[.]sh	Exfiltration hosting service
Domain	linkedinsso[.]com	Phishing domain
Domain	mgmresorts-okta[.]com	Phishing domain
IP	99.25.84[.]9	Observed IP in campaigns
IP	144.76.136[.]153	Observed IP in campaigns
Ransomware	BlackCat/ALPHV	Used by group
Ransomware	RansomHub	Used by group
Ransomware	Qilin	Used by group

EXTERNAL REFERENCES OUTSIDE OF CYBERINT

1. https://blog.netwrix.com/mgm-cyber-attack
2. https://www.reuters.com/technology/cybersecurity/iag-flags-air-europas-customers-personal-data-leak-wsj-reports-2024-03-21/
3. https://apnews.com/article/japan-jal-cyberattack-flights-travel-04fbd4848f3015a77057339a5c90ca32
4. https://apnews.com/article/seattle-airport-cyberattack-ransomware-rhysida-95cd980a9f45112f0fdce488233eec9c
5. https://www.theguardian.com/uk-news/article/2024/sep/02/transport-for-london-dealing-with-cyber-attack
6. https://www.voyageursdumonde.fr/voyage-sur-mesure/Img/institutionnel/info-fi/data/2023/PR_Voyageurs_du_Monde_17.5.2023.pdf
7. https://www.skynews.com.au/australia-news/australian-travel-agency-hit-by-data-breach-leaking-passport-and-travel-details-of-thousands-of-customers/news-story/73072684e13a253e315d326b916280c1
8. https://icsstrive.com/incident/aerticket-suffers-cyberattack-causing-technical-failures/
9. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
10. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
11. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108
12. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
13. https://www.sentinelone.com/anthology/inc-ransom/
14. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm