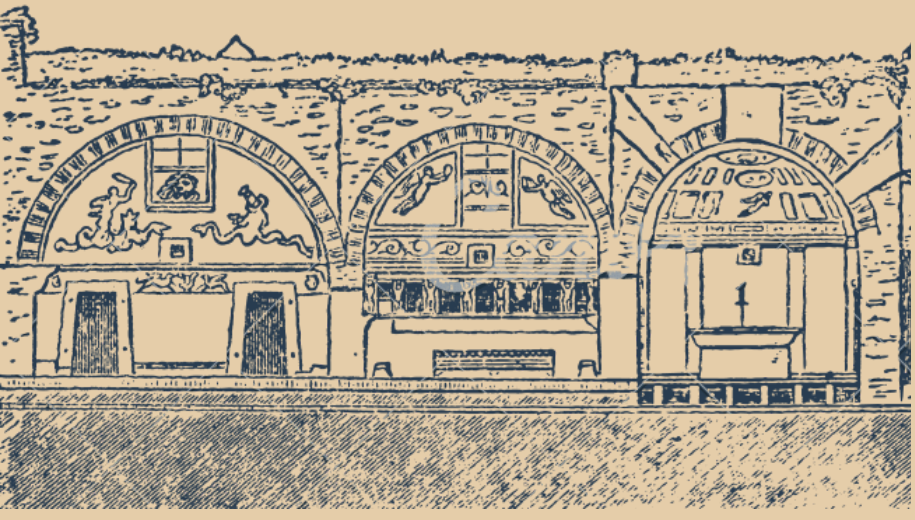
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 05 JULY – 11 JULY 2026



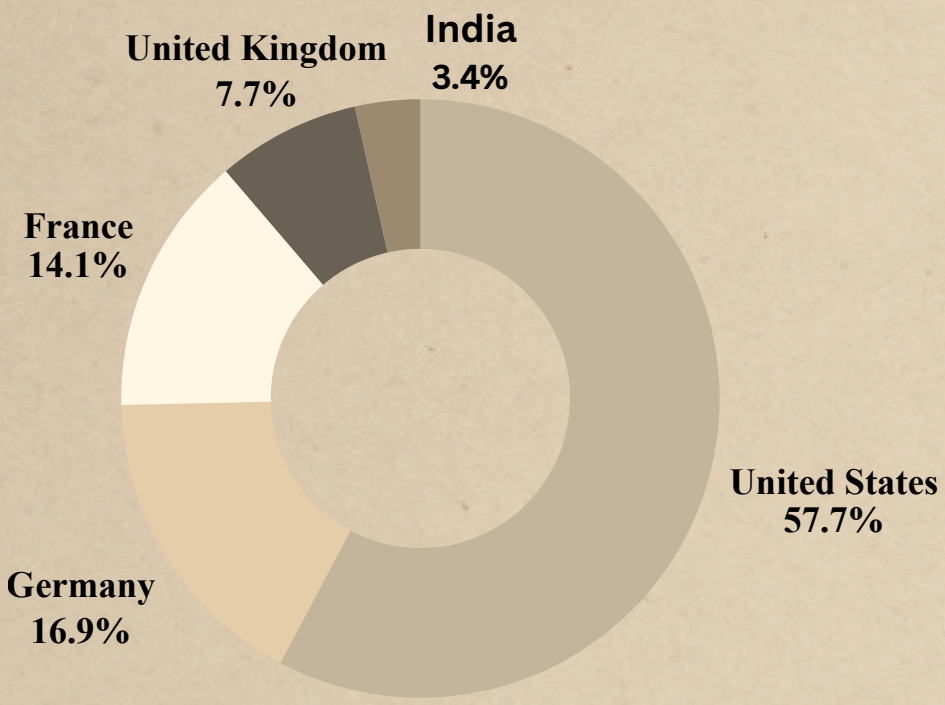
GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 05 JULY - 11 JULY 2026

Overview

This weekly report provides an overview of global data breach activity linked to threat groups. It focuses on exposure patterns, threat actor activity, and key trends observed across industries and geographies.

Geographic Distribution



Key Highlights

- The majority of incidents were linked to ransomware and data extortion activity, highlighting the continued dominance of financially motivated cyber threats.
- Threat groups such as **Deadlock**, **The Gentlemen**, **Qilin**, and **LockBit** were most frequently observed, indicating sustained and coordinated attack campaigns.

Most Targeted Sector: IT / Technology

Total Breaches Observed: 291

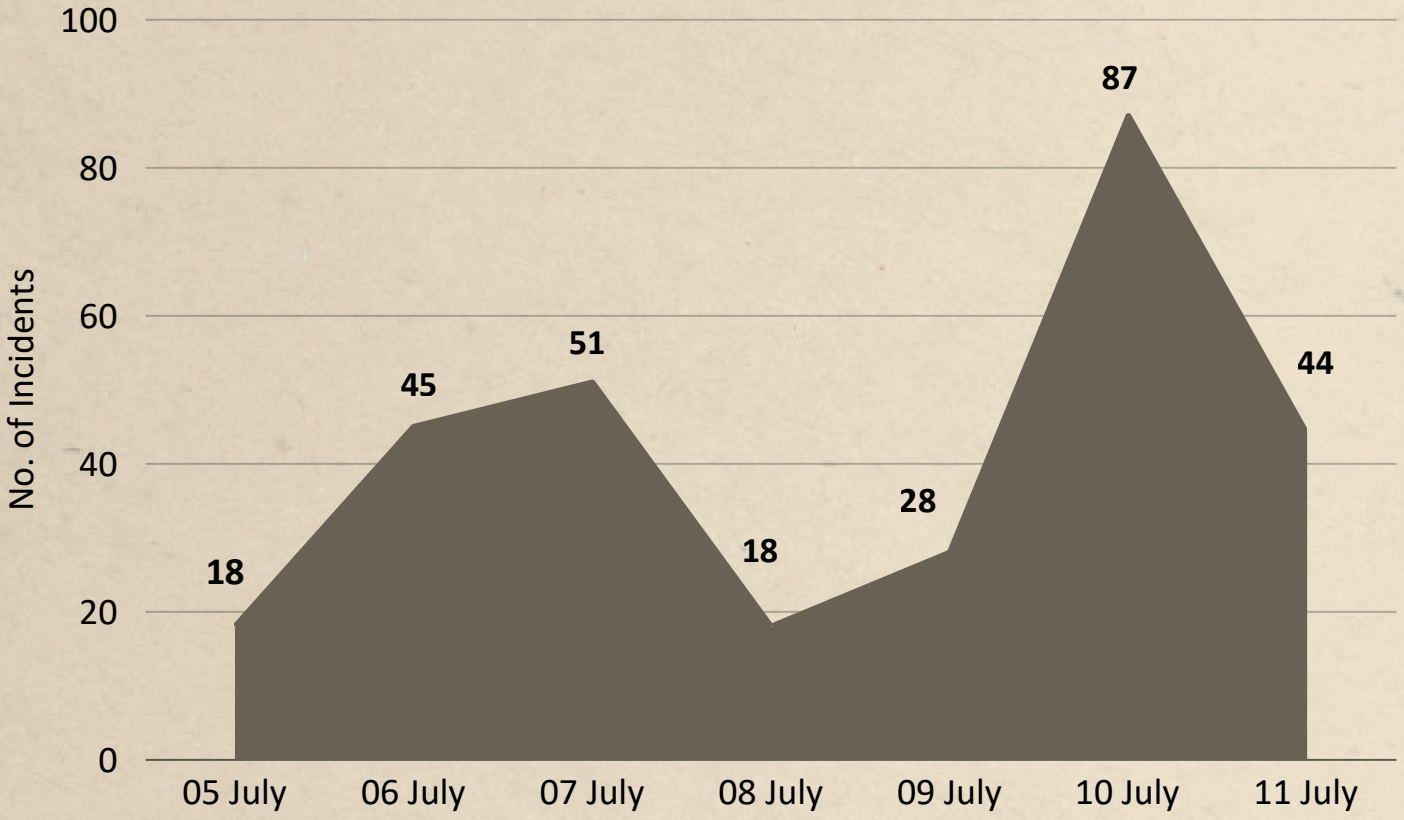
Ransomware-linked breaches: 83.5%

Countries Affected: 57

GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 05 JULY - 11 JULY 2026

Breach Over time

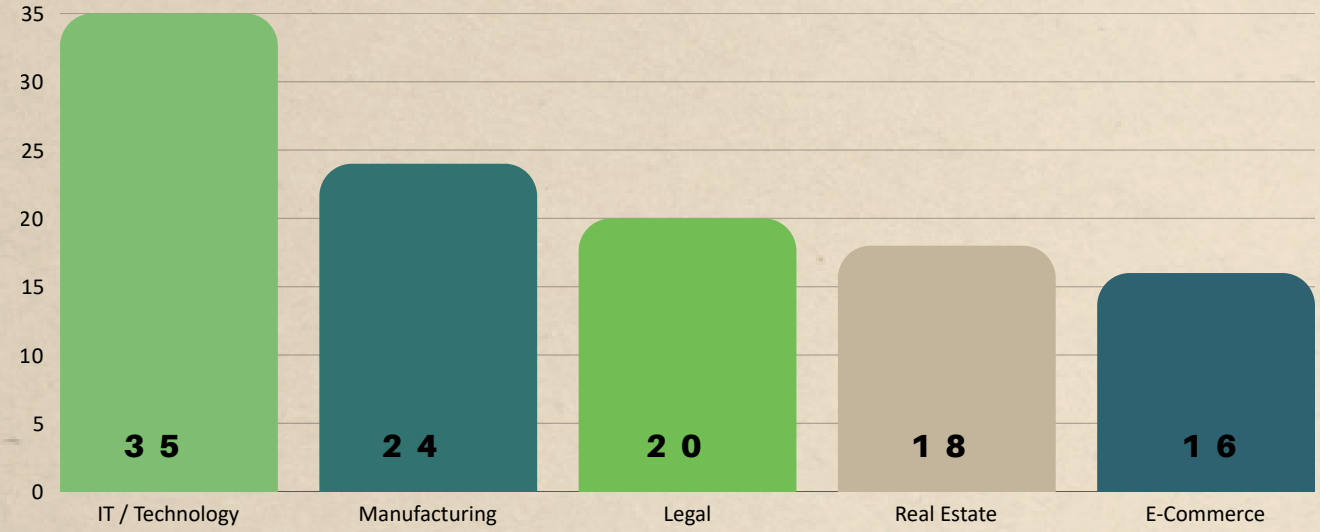


- Breach activity fluctuated throughout the period, with July 10, recording the highest spike at 87 reported incidents.
- A sharp rise was observed between July 05 and July 07, peaking at 51 incidents on July 07, indicating intensified disclosure or attack activity.
- July 05 and july 08 reported the lowest number of incidents, with only 18 breaches observed.
- Overall, the trend reflects irregular but high-impact surges, followed by short periods of decline and stabilization.

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:05JULY-11JULY 2026

Affected Sectors



Industry Highlights

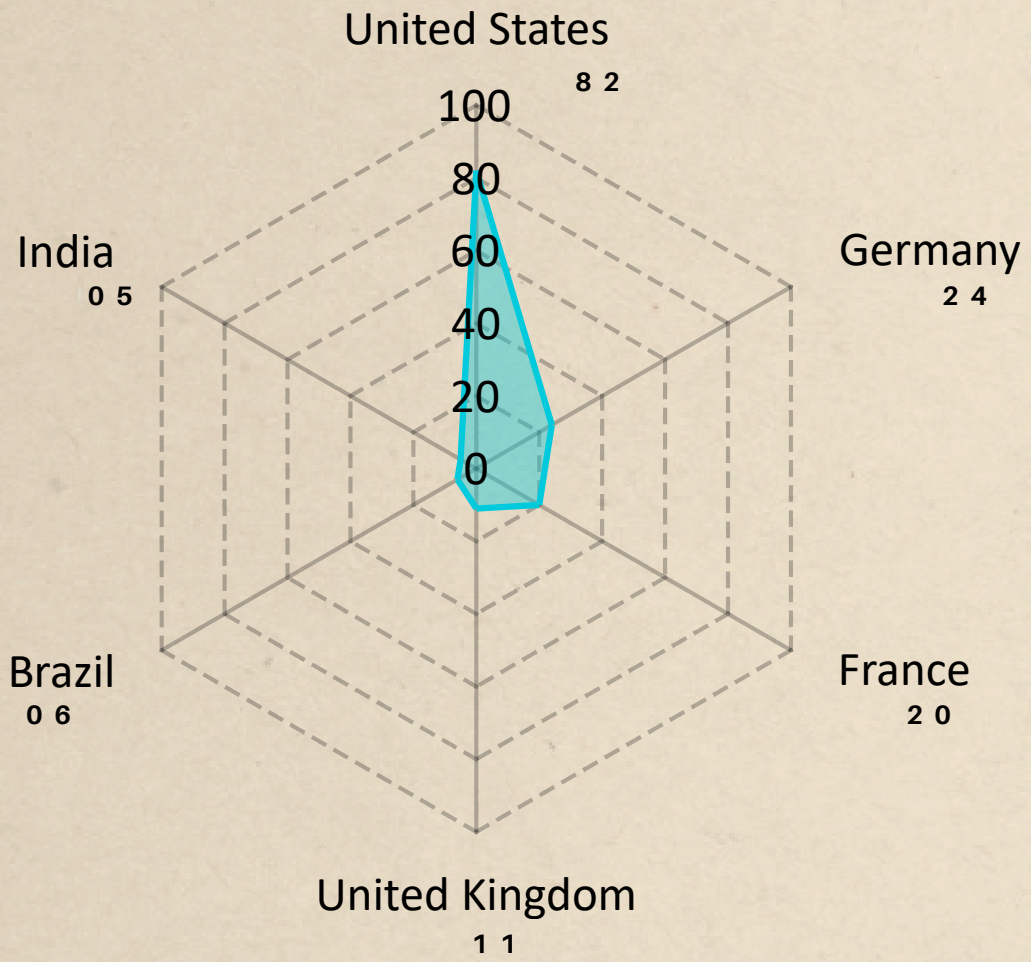
- **IT / Technology: 35+ incidents (highest targeted sector)**
- **Manufacturing & Engineering: 24+ incidents**
- **Legal : 20+ incidents**
- **Real Estate : 18+ incidents**
- **E-Commerce : 16+ incidents**

Industries Insight: Technology organizations recorded the highest number of incidents during this period, followed by manufacturing, finance, construction, and retail. These sectors remain attractive targets due to their extensive digital infrastructure, valuable business data, and critical operational dependencies.rastructure, extensive customer data, and business-critical operations.

GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 05 JULY - 11 JULY 2026

Affected Countries



Actor Distribution

Ransomware dominates the threat landscape with 243+ incidents, far outpacing 48 non-ransomware cases, making it the most prevalent and impactful attack type.

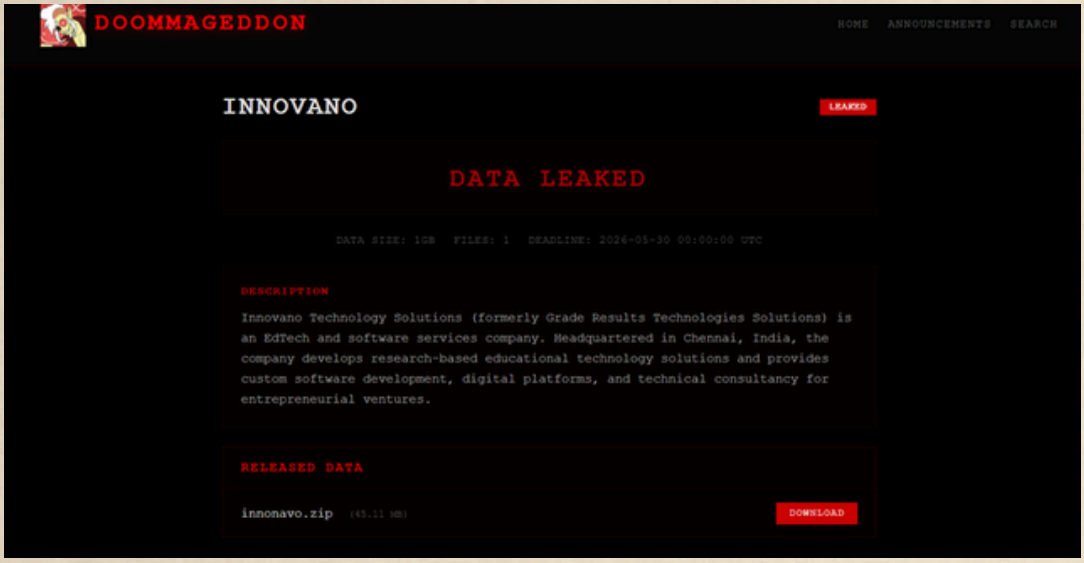
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:05JULY-11JULY 2026

Innovano Breach Incident

On July 06, 2026, **Innovano,** a IT company suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector : IT
Threat Group (Ransomware) : Doommageddon
Data Sold: 1 GB
Country: India



Key Highlights

- **Data Exposure:** Alleged 1 GB of Innovano Technology Solutions data was published on the DOOMMAGEDDON leak site.
- **Threat Group:** Linked to **DOOMMAGEDDON**
- **Source & Risk:** The leak reportedly includes an innonavo.zip archive made available for download.
- **Threat Activity:** Public disclosure of alleged stolen company data as part of a data leak campaign..
- **Threat Level:** Medium due to the potential exposure of corporate information.

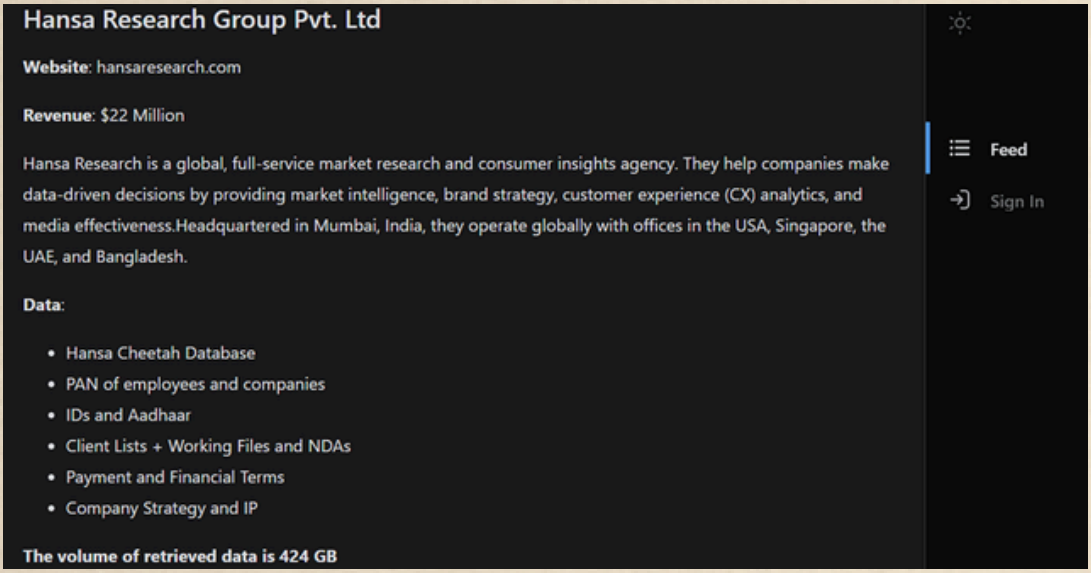
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:05JULY-11JULY 2026

Hansa Research Group Pvt. Ltd Breach Incident

On July 06, 2026, **Hansa Research Group Pvt. Ltd,** a Communication / Marketing company suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Communication / Marketing
Threat Group (Ransomware) : morpheus
Data Sold : 424 GB
Country: India



Key Highlights

- **Data Exposure:** Alleged 424 GB of Hansa Research Group Pvt. Ltd. data was published on a leak site.
- **Threat Group :** Posted by **Morpheus**
- **Source & Risk:** The leak reportedly includes Aadhaar IDs, PAN details, client lists, NDAs, financial records, and company strategy data.
- **Threat Activity :** Public disclosure of alleged stolen corporate and personal data as part of a data extortion campaign.
- **Threat Level:** Critical due to the exposure of sensitive personal, financial, and confidential business information.

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:05JULY-11JULY 2026

CSIR Structural Engineering Research Centre Breach Incident

On July 07, 2026, **CSIR Structural Engineering Research Centre**., Research company suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Research
Threat Group (Ransomware) : thegentlemen
Data Sold : 83 Bytes
Country : India

Key Highlights

- **Data Exposure:** Alleged CSIR Structural Engineering Research Centre data was listed on a leak site.
- **Threat Group :** Linked to **thegentlemen**
- **Source & Risk:** A contact file (CONTACT_BUY_DATA.txt) indicates the data is being offered for sale.
- **Threat Activity:** Alleged sale of stolen organizational data as part of a data extortion campaign.
- **Threat Level:** Medium due to the potential exposure of institutional information.

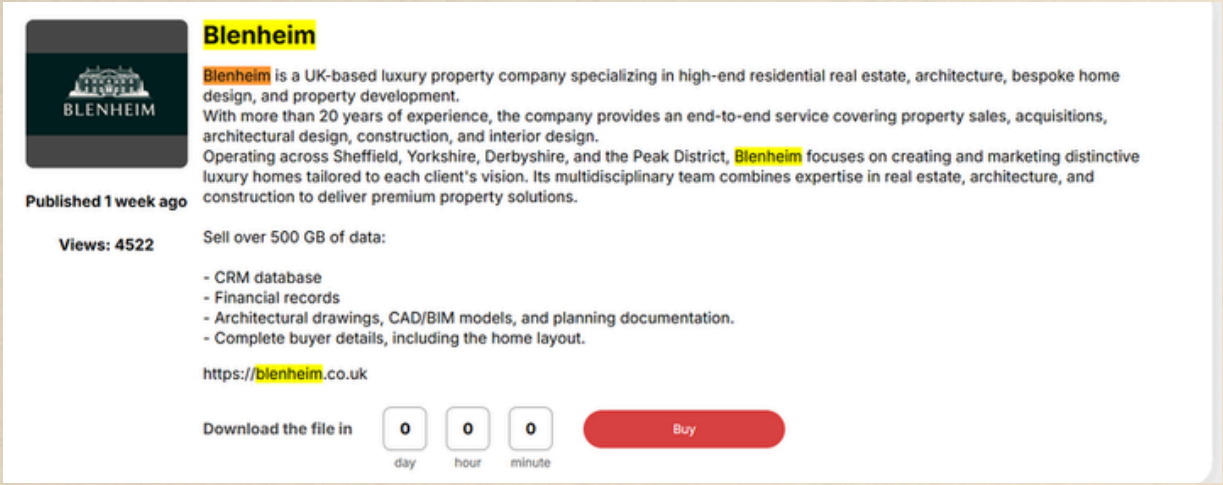
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:05JULY-11JULY 2026

Blenheim Breach Incident

On July 06, 2026, **Blenheim,** a Hospitality company, suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector : Hospitality
Threat Group (Ransomware) : spacebears
Data Sold: 500 GB
Country : United Kingdom



Key Highlights

- **Data Exposure:** Alleged 500+ GB of Blenheim data was offered for sale on a leak site.
- **Threat Activity:** Alleged sale of stolen corporate and customer data as part of a data extortion campaign.
- **Threat Group :** Linked to **spacebears**
- **Source & Risk:** The dataset reportedly includes CRM databases, financial records, CAD/BIM drawings, planning documents, and buyer information.
- **Threat Level:** Critical due to the exposure of financial, customer, and sensitive architectural data.

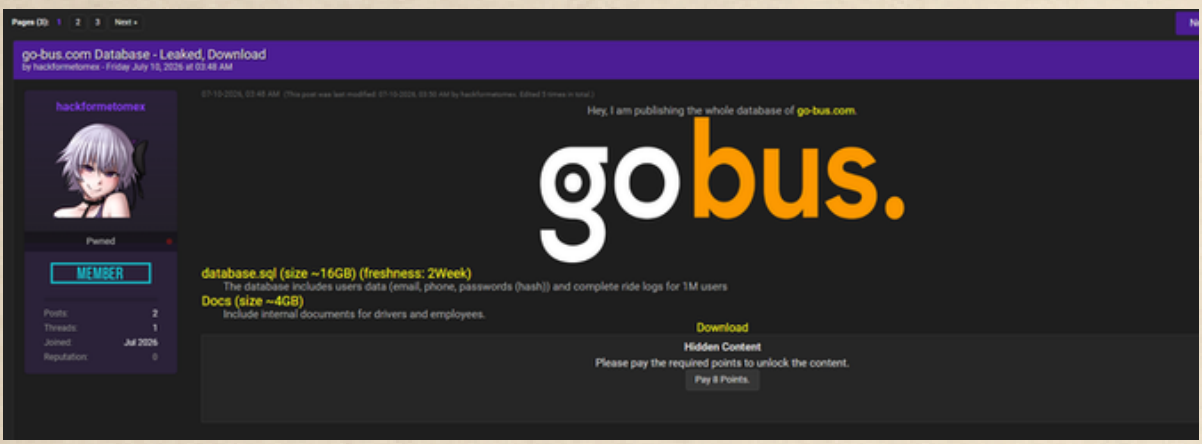
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:05JULY-11JULY 2026

Go Bus Breach Incident

On July 10, 2026, **Go Bus,** a Travel & Mobility company suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Travel & Mobility
Threat Actor : hackformetomex
Data Sold: 4GB
Country : Egypt



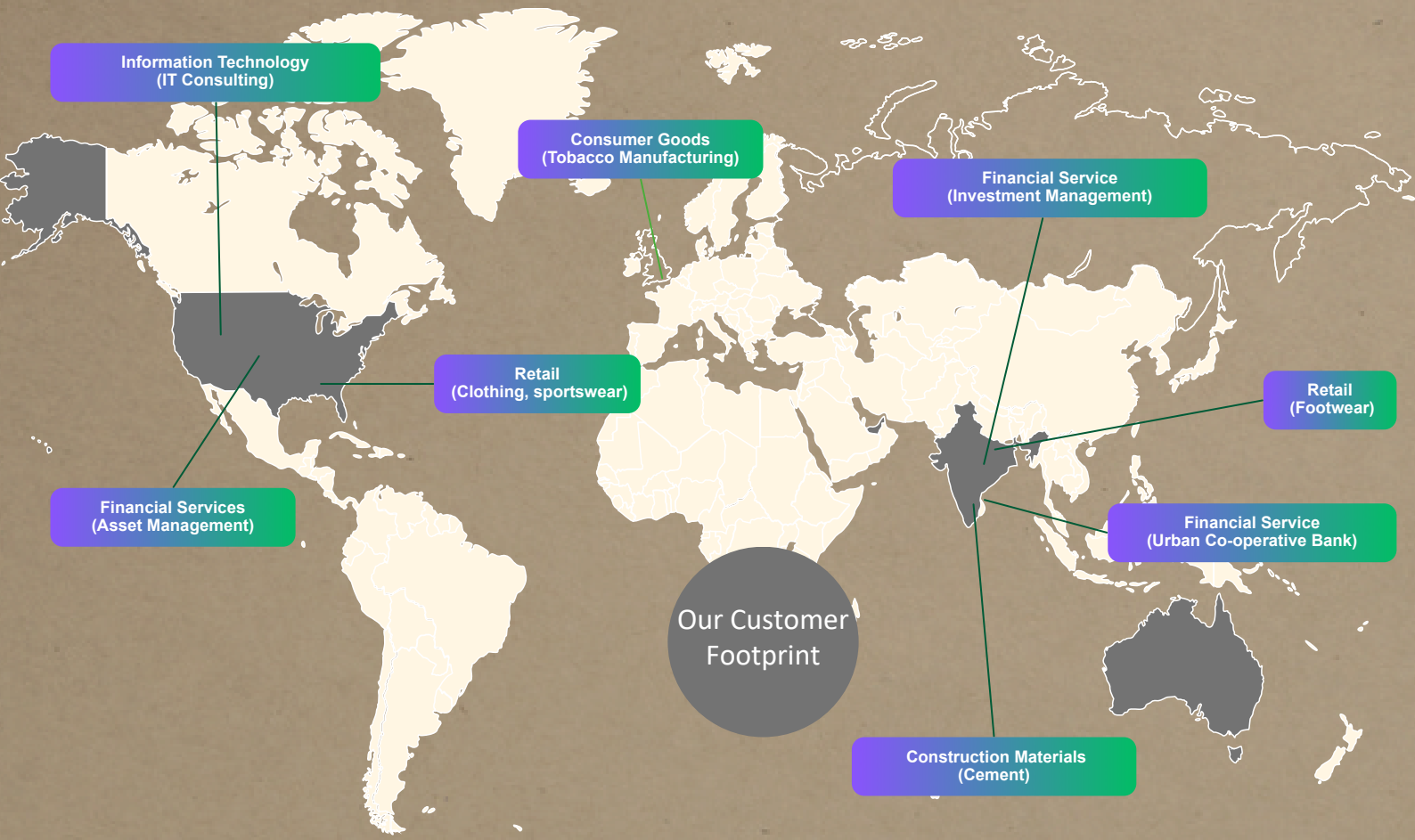
Key Highlights

- **Data Exposure:** Alleged 20 GB of go-bus.com data was published on a leak site, including a 16 GB database and 4 GB of documents.
- **Threat Actor:** Linked to **hackformetomex**
- **Source & Risk:** The leak reportedly contains emails, phone numbers, password hashes, ride logs, and internal employee documents affecting 1 million users.
- **Threat Activity:** Public disclosure of alleged stolen data as part of a data extortion campaign.
- **Threat Level:** Critical due to the exposure of customer credentials, personal data, and internal corporate documents.

About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio

Secure Cloud WL

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

We create secure cloud environments, automate Cloud SecOps & manage it.

24x7 Monitoring

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

When it comes to SOC Monitoring & Response, we cover all aspects of it

Vuln Mgmt

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuin Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

Program designed VAPT Engagement to enhance protection & reduce attack surface

Threat Intel

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

We take threat intel maintenance, keep, usage & application to next level.

Data & Privacy

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

Data and privacy are two considerations, we design, implement it & run compliances

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995