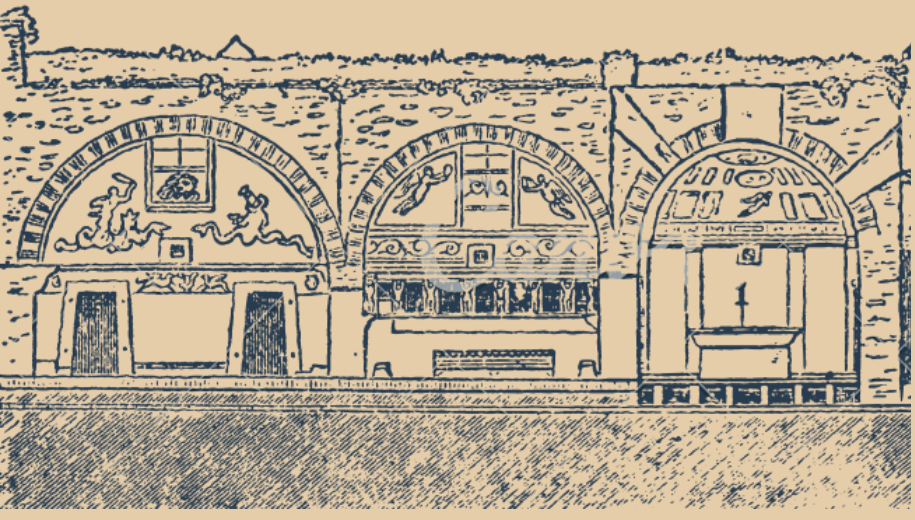
CASTELLUM LABS

# WEEKLY DIGEST

## GLOBAL BREACHES & RANSOMWARE VICTIMS

**REPORTING PERIOD: 17 MAY – 23 MAY 2026**



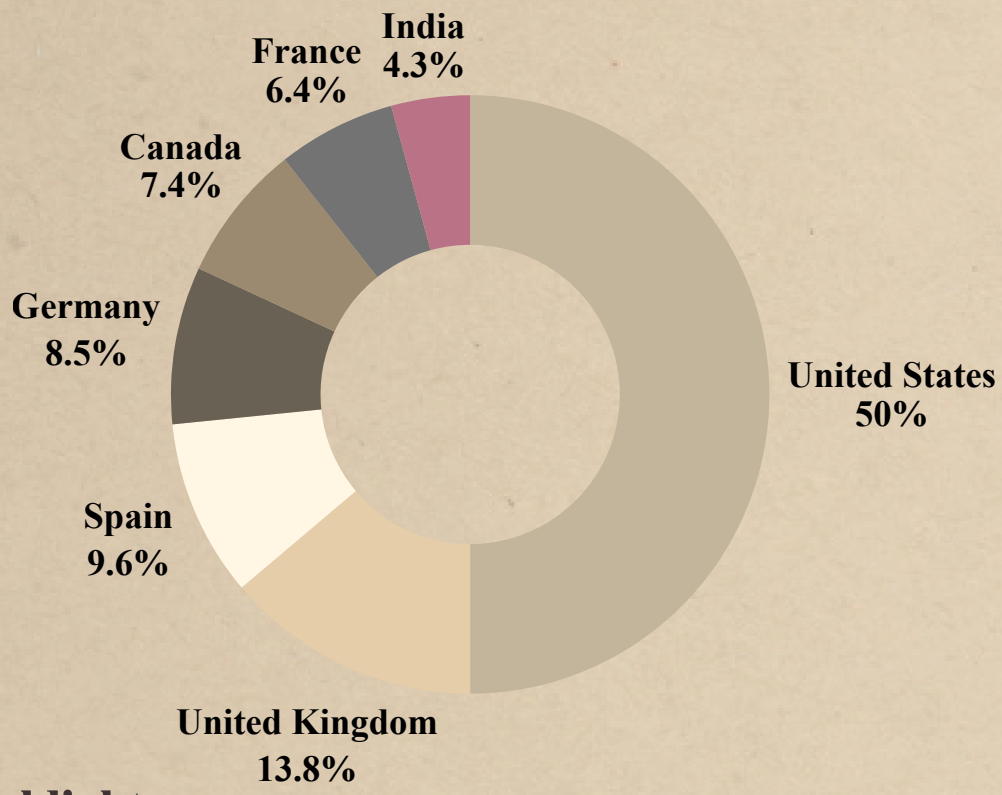
# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:17 MAY - 23 MAY 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 associated with ransomware and data extortion operations, underscoring the continued activity of financially motivated threat actors.
- Groups such as **Qilin**, **Nova**, **Akira**, and **APT73** were repeatedly identified, indicating sustained and coordinated cyberattack campaigns.

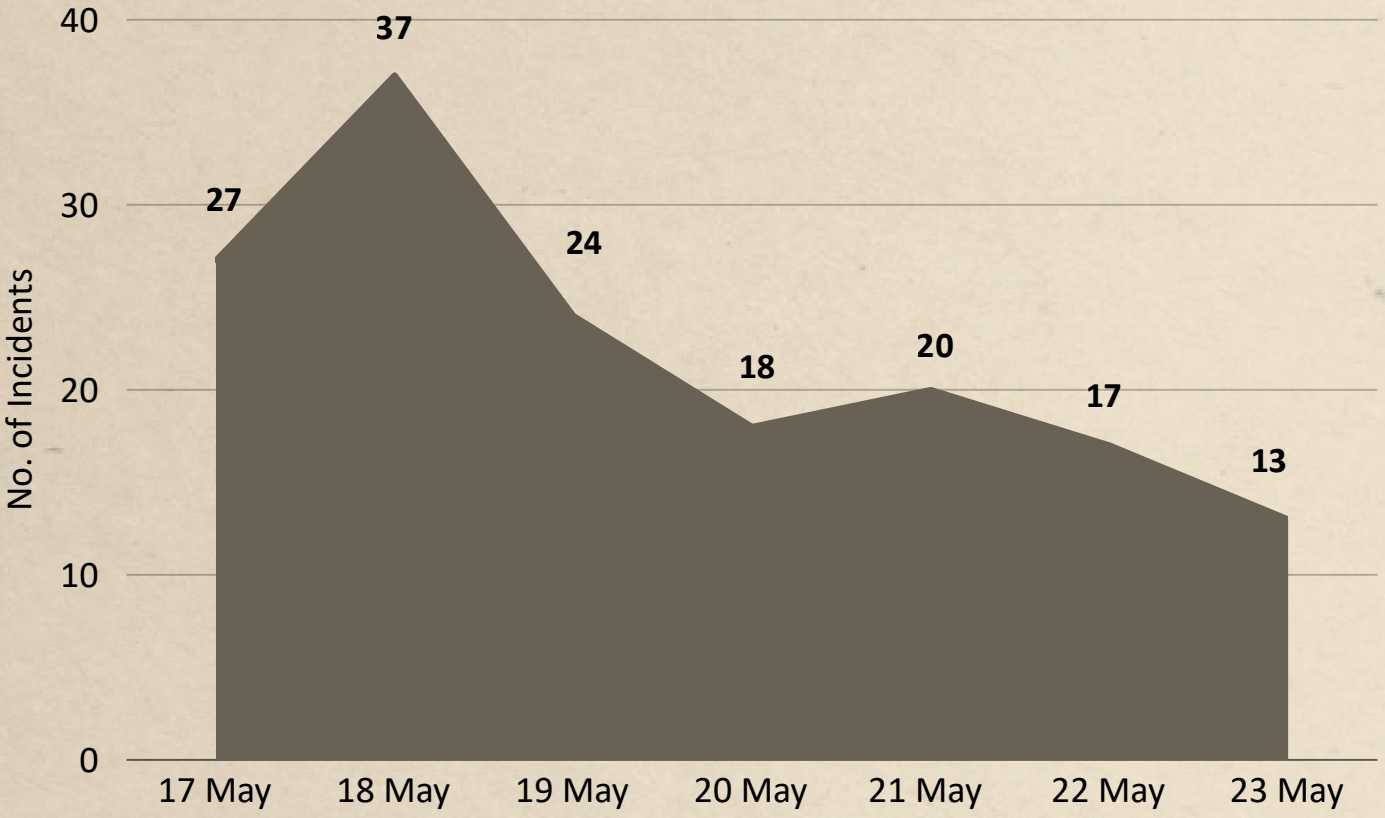
**Most Targeted Sector:** Manufacturing
**Ransomware-linked breaches:** 87.8%

**Total Breaches Observed:** 156
**Countries Affected:** 40

# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:17 MAY - 23 MAY 2026

## Breach Over time

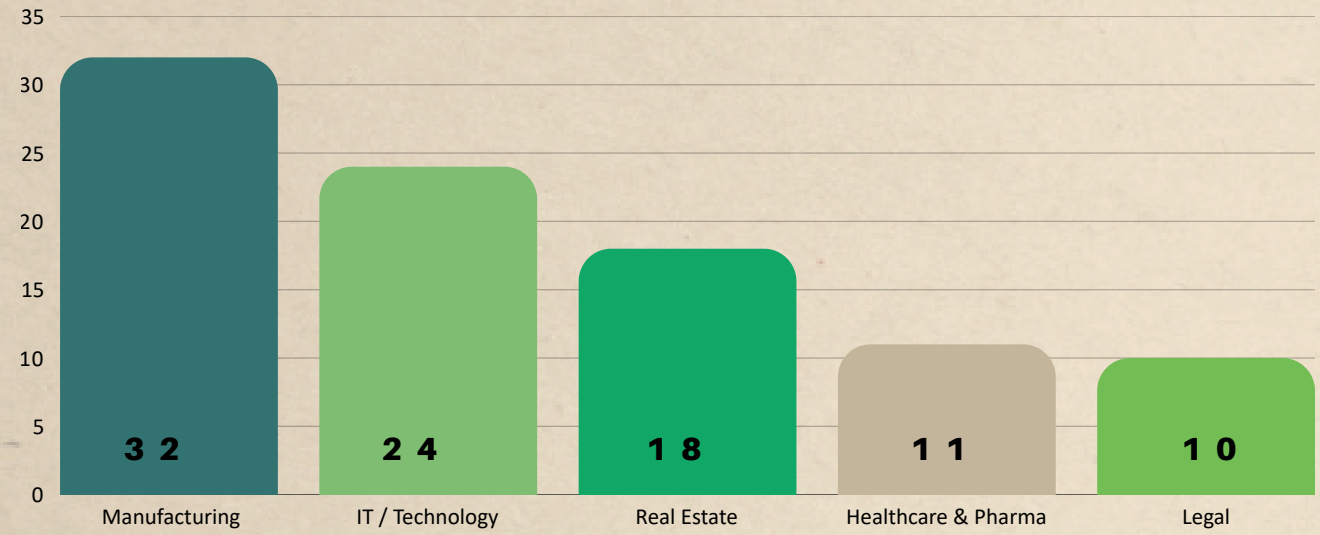



- Breach activity fluctuated throughout the period, with May 18 recording the highest spike at 37 reported incidents.
- A sharp rise was observed between May 17 and May 19, peaking at 27 incidents on May 17, indicating intensified disclosure or attack activity.
- May 23 reported the lowest number of incidents, with only 13 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: 17 MAY - 23 MAY 2026

## Affected Sectors




## Industry Highlights

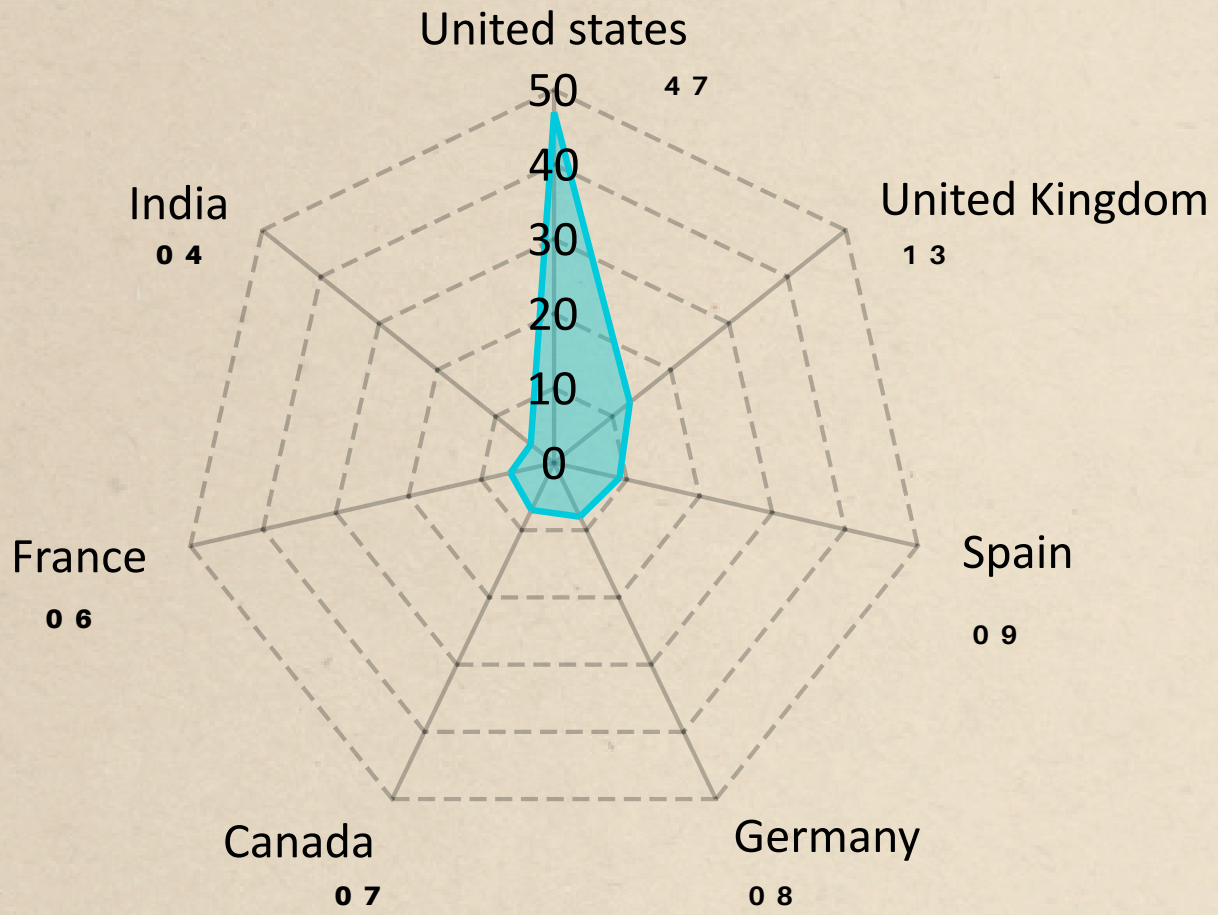
- **Manufacturing & Engineering: 32+ incidents (highest targeted sector)**
- **IT / Technology: 24+ incidents (high exposure due to digital infrastructure)**
- **Real State: 18+ incidents**
- **Healthcare & Pharma: 11+ incidents**
- **Finance / Legal / Insurance: 10+ incidents**

**Industries Insight:** Manufacturing and technology sectors remained the primary focus for threat actors, while construction, healthcare, and financial organizations also faced sustained targeting due to operational dependence and sensitive data exposure.

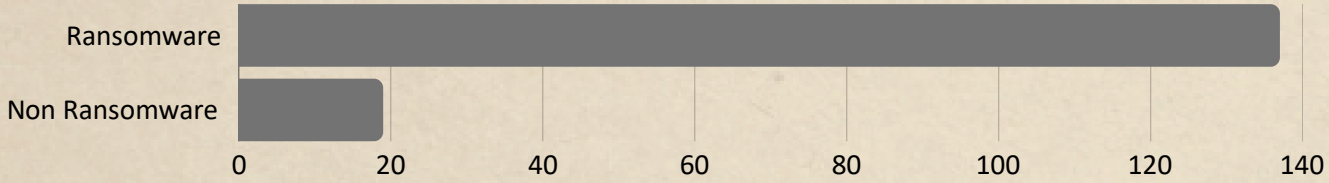
# GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:17 MAY - 23 MAY 2026

## Affected Countries




## Actor Distribution




Ransomware dominates the threat landscape with 137+ incidents, far outpacing 19 non-ransomware cases, making it the most prevalent and impactful attack type.

# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 17 MAY - 23 MAY 2026

## Venture Yours Breach Incident

On May 18, 2026, a US company Venture Yours suffered a significant data breach during the week, involving potentially sensitive information.

**Company Sector:** **PropTech / Vacation Rental Management**
**Threat Actor :** **zSenior**
**Data Sold:** **64 GB**


## Key Highlights

- **Data Exposure:** Approx 25.5M CSV records and 70K+ files reportedly leaked, including KYC documents, booking details, and customer PII
- **Threat Actor:** Linked to zSenior / BlavoForums
- **Threat Activity:** Shared on underground forum; exposed data allegedly includes driver licenses, rental agreements, emails, and phone numbers
- **Threat Level:** Critical non-ransomware breach with risks of identity theft, fraud, customer privacy violations, and unauthorized account misuse

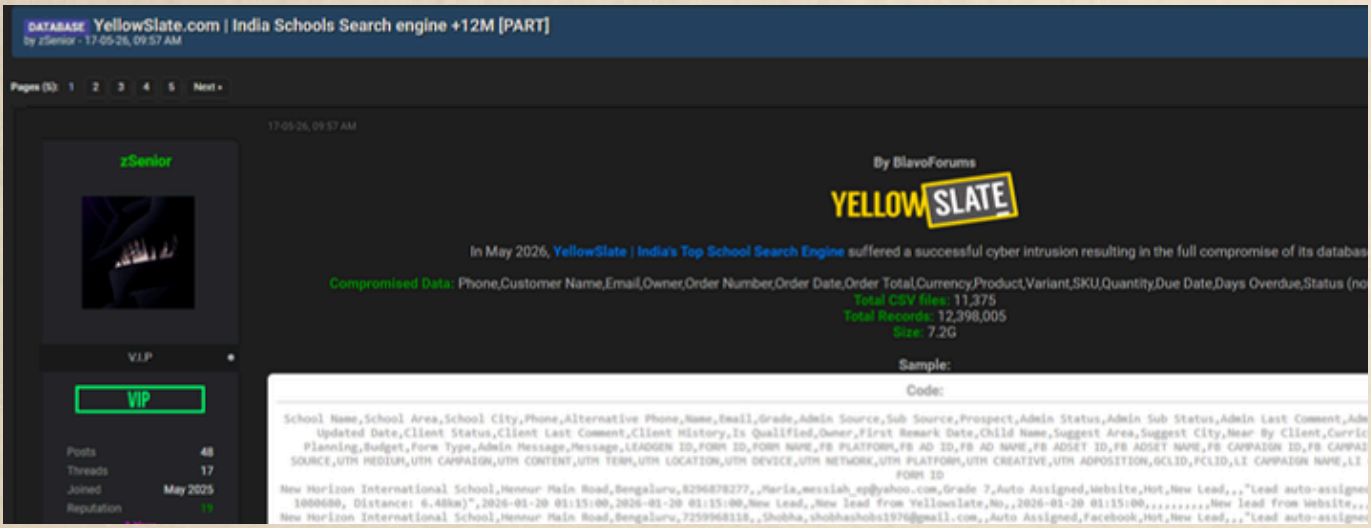
# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 17 MAY - 23 MAY 2026

## Yellow Slate Breach Incident

On May 17, 2026, a India company Yellow Slate suffered a significant data breach during the week, involving potentially sensitive information.

**Company Sector:** EdTech
**Threat Actor :** zSenior
**Data Sold:** 7.2GB




## Key Highlights

- **Data Exposure:** Approx 12.3M records reportedly leaked from an Indian school search platform database
- **Threat Actor:** Linked to zSenior / BlavoForums
- **Threat Activity :** Shared on underground forum; exposed data allegedly includes phone numbers, emails, customer details, and school-related records
- **Threat Level:** Large-scale non-ransomware breach with risks of spam campaigns, data misuse, unauthorized profiling, and privacy violations

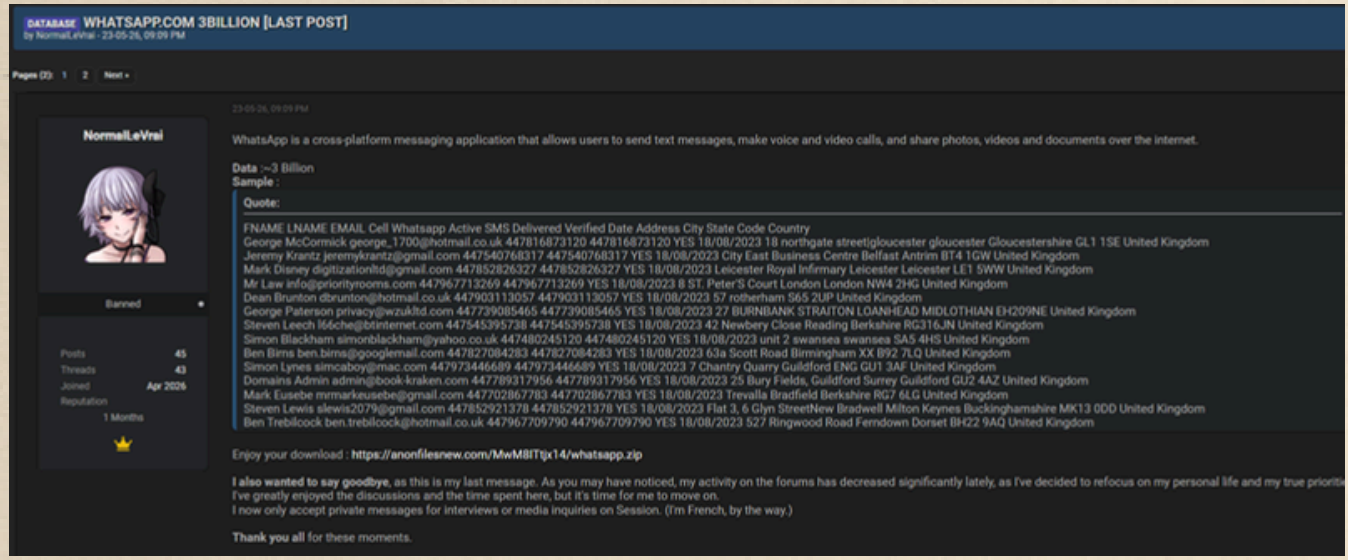
# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:17 MAY - 23 MAY 2026

## WhatsApp LLC  Breach Incident

On May 23, 2026, a USA company WhatsApp LLC suffered a significant data breach during the week, involving potentially sensitive information..

**Company Sector:** Technology
**Threat Actor :** NormalLeVrai
**Data Sold:** 3.78 GB




## Key Highlights

- **Data Exposure:** Alleged leak claims exposure of approximately 3 billion WhatsApp-related records containing phone numbers, emails, and address details
- **Threat Actor:** Linked to NormalLeVrai
- **Threat Activity:** Shared on underground forum with downloadable archive references and sample records posted publicly
- **Threat Level:** Massive non-ransomware data exposure with high risks of phishing, spam campaigns, identity misuse, and large-scale social engineering attacks

# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:17 MAY - 23 MAY 2026

## Universidad del Quindío Breach Incident

On May 20, 2026, a Colombia company Universidad del Quindío suffered a significant data breach during the week, involving potentially sensitive information..

**Company Sector:** Higher Education
**Threat Actor :** Skull1172
**Data Sold:** 3.26 GB


## Key Highlights

- **Data Exposure:** Approx 3.26GB JSON database reportedly leaked, containing emails, passwords, full names, and administrative credential data
- **Threat Activity:** Alleged exposure impacts multiple academic departments and administrative systems of Universidad del Quindío
- **Threat Actor:** Linked to Skull1172 / EsqueleSquad
- **Threat Level:** High-risk academic data breach with potential for credential compromise, phishing attacks, and unauthorized institutional access

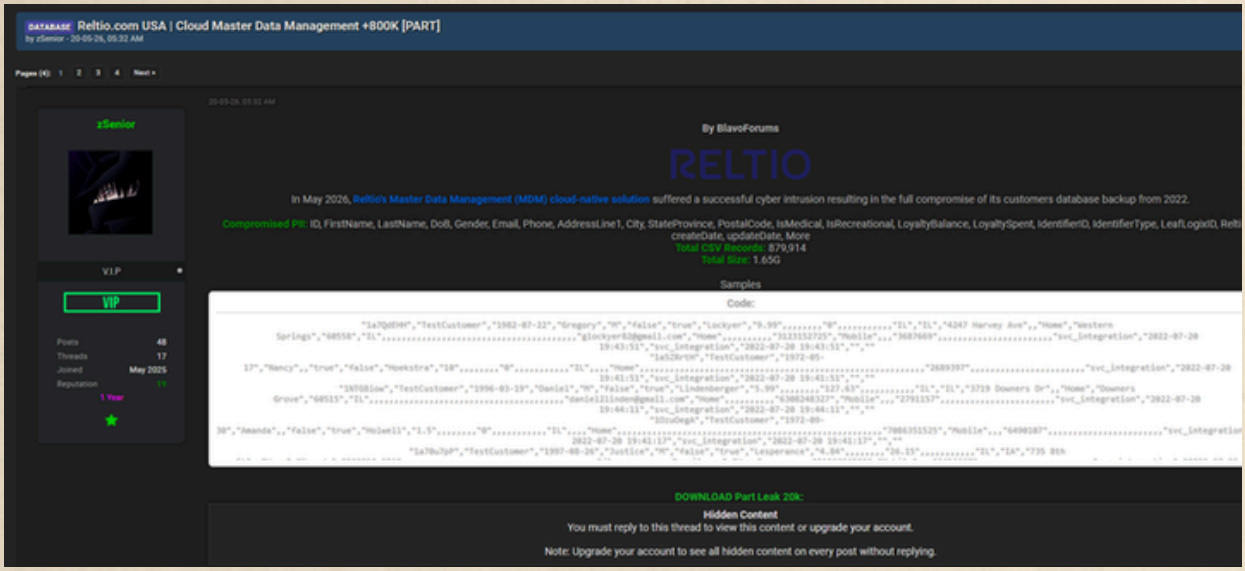
# GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 17 MAY - 23MAY 2026

## Reltio Breach Incident

On May 20, 2026, a USA company Reltio suffered a significant data breach during the week, involving potentially sensitive information..

**Company Sector:** Enterprise Tech
**Threat Actor :** zSenior
**Data Sold:** 1.65 GB



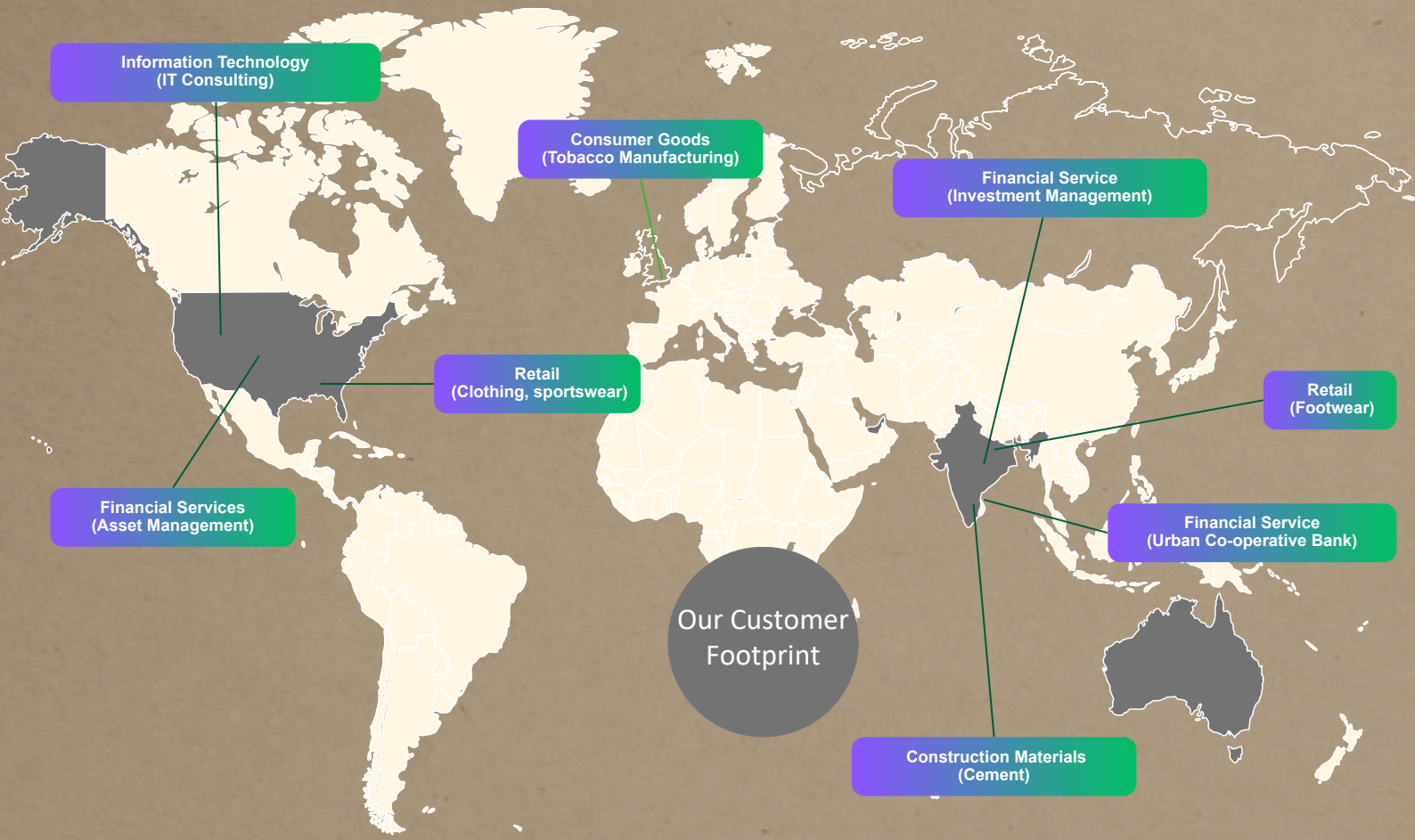

## Key Highlights

- **Data Exposure:** Approx 1.65 GB of data reportedly leaked, includingID, FirstName, LastName, DoB, Gender, Email, Phone, AddressLine1, City.
- **Threat Actor:** Linked to zSenior / BlavoForums
- **Threat Activity:** Shared on underground forum; alleged exposure includes corporate intelligence and employee personal documents
- **Threat Level:** Critical ransomware-related breach with risks of corporate espionage, employee data misuse, and operational disruption

# 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