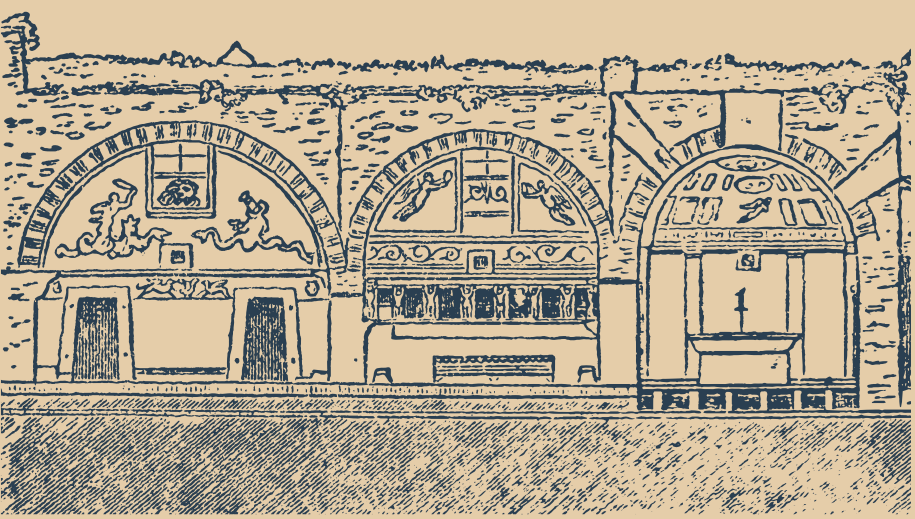
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 03 MAY – 16 MAY 2026



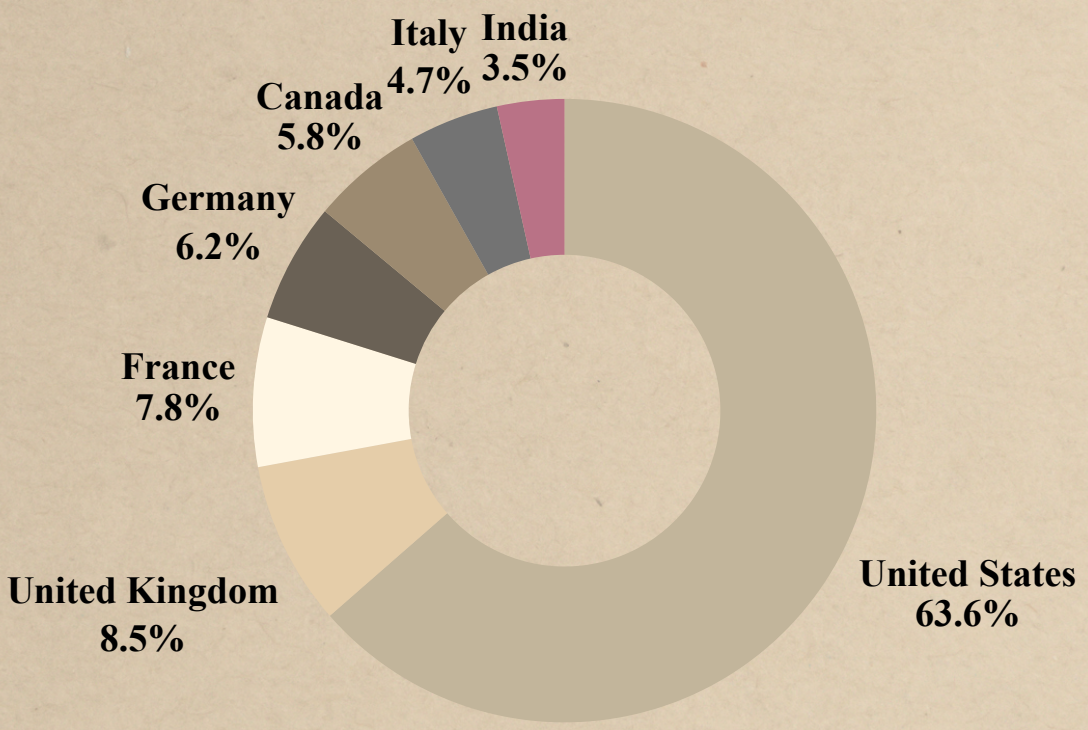
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:03 MAY - 16 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 linked to ransomware and data extortion activity, highlighting the continued prevalence of financially motivated cyberattacks.
- Threat groups such as **The Gentlemen**, **Qilin**, **Akira**, and **incransom** were most frequently observed, indicating persistent and coordinated attack campaigns.

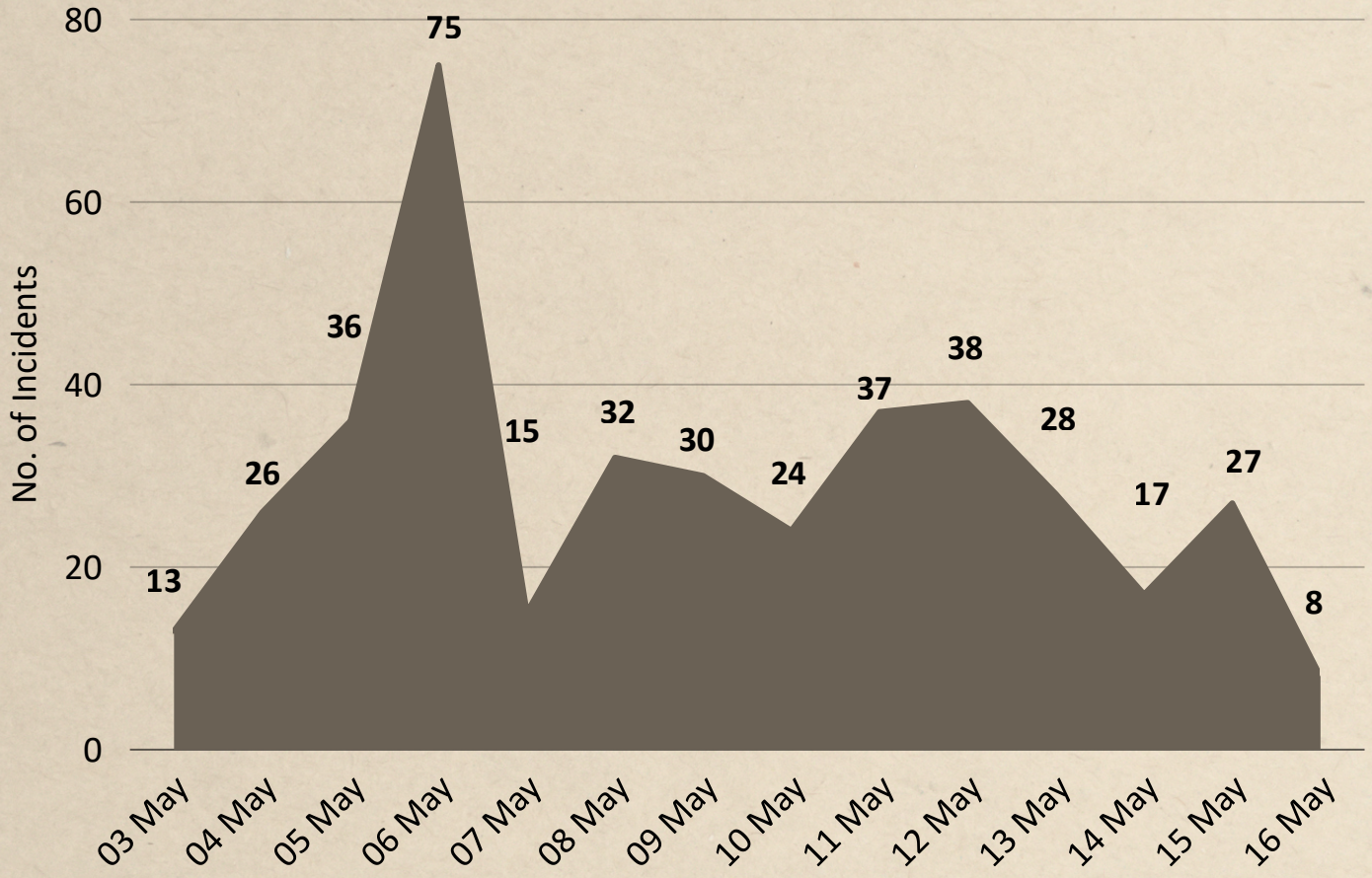
Most Targeted Sector: Manufacturing
Ransomware-linked breaches: 89.2%

Total Breaches Observed: 406
Countries Affected: 63

GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:03 MAY - 16 MAY 2026

Breach Over time

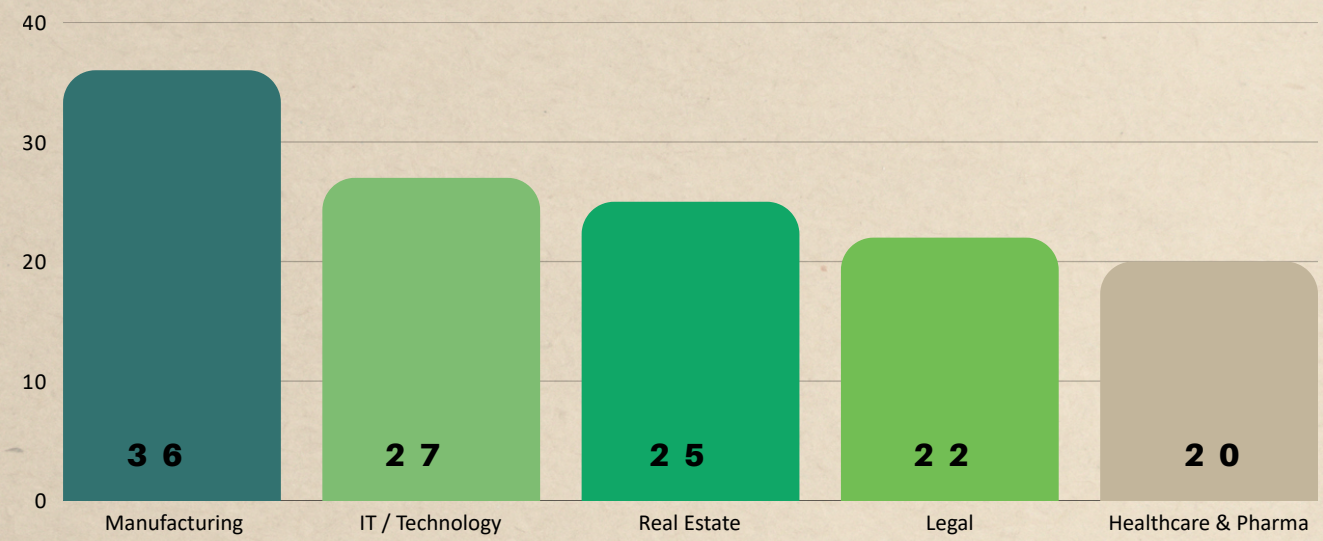


- Breach activity fluctuated throughout the period, with May 06 recording the highest spike at 75 reported incidents.
- A sharp rise was observed between May 10 and May 12, peaking at 38 incidents on May 12, indicating intensified disclosure or attack activity.
- May 16 reported the lowest number of incidents, with only 08 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:03 MAY - 16 MAY 2026

Affected Sectors



Industry Highlights

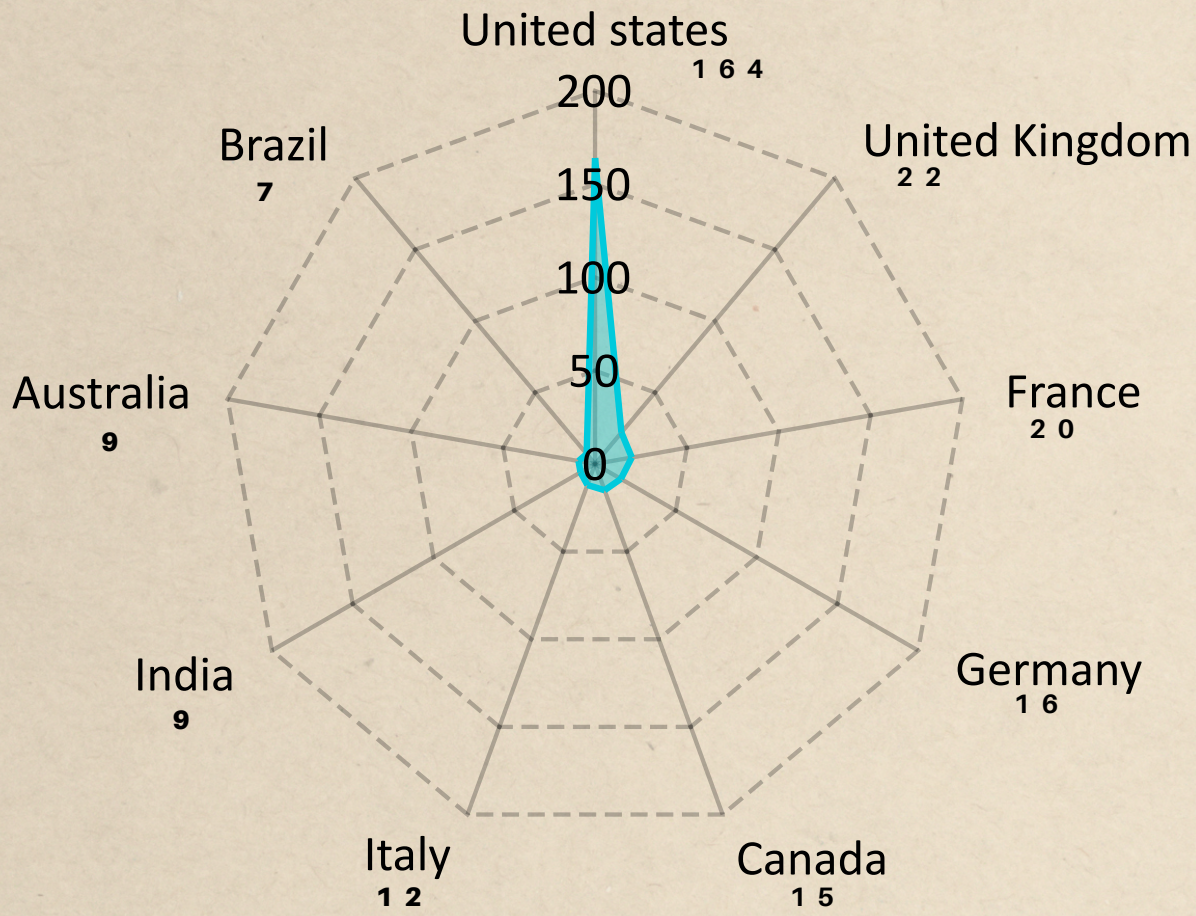
- **Manufacturing & Engineering: 36+ incidents (highest targeted sector)**
- **IT / Technology: 27+ incidents (high exposure due to digital infrastructure)**
- **Real State: 25+ incidents**
- **Finance / Legal / Insurance: 22+ incidents**
- **Healthcare & Pharma: 20+ incidents**

Industries Insight: Manufacturing, technology, construction, finance, and healthcare remained the most frequently targeted sectors, reflecting continued focus on operationally critical and data-rich industries.

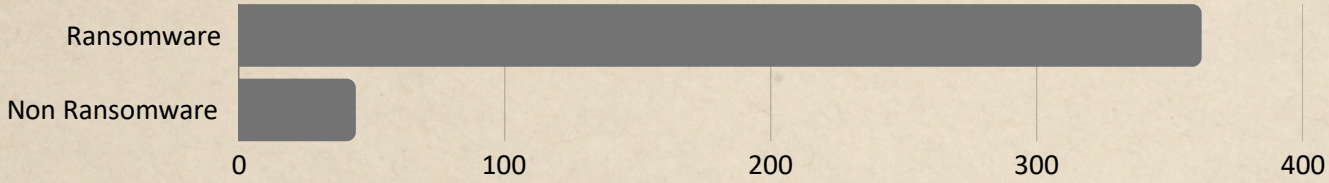
GLOBAL DATA BREACH REPORT

REPORTING PERIOD:03 MAY - 16 MAY 2026

Affected Countries



Actor Distribution



Ransomware dominates the threat landscape with 362+ incidents, far outpacing 44 non-ransomware cases, making it the most prevalent and impactful attack type.

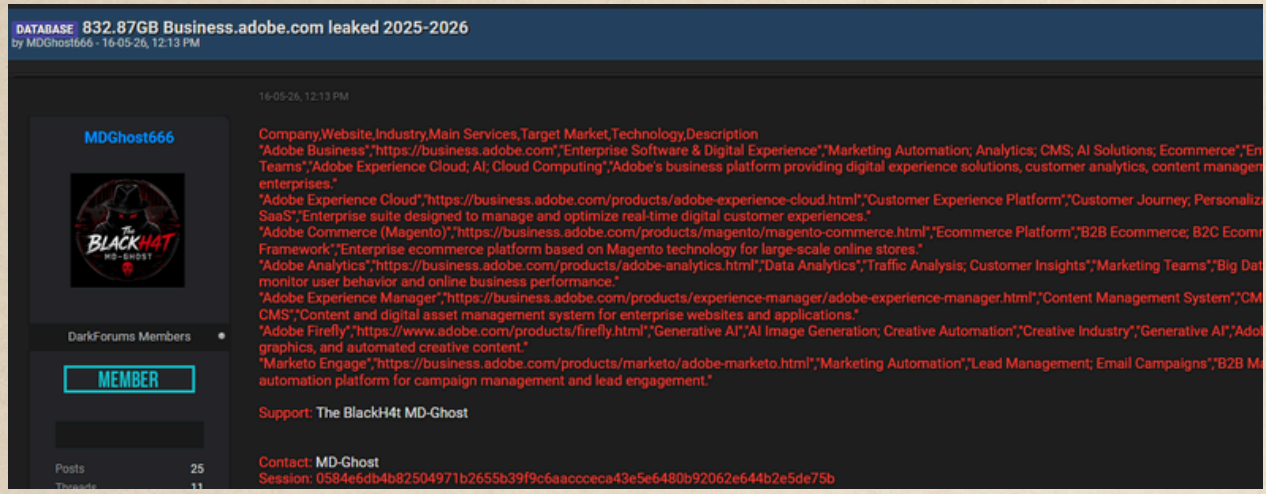
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 03 MAY - 16 MAY 2026

Adobe Inc. Breach Incident

On May 16, 2026, a US company Adobe Inc. suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: **Enterprise Software / SaaS / Marketing Analytics**
Threat Actor : **MDGhost666**
Data Sold: **832.87 GB**



Key Highlights

- **Data Exposure:** Massive leak claim involving 832.87GB of Adobe business-related data spanning 2025–2026
- **Threat Actor:** Linked to MDGhost666 (The BlackH4t MD-Ghost)
- **Threat Activity:** Posted on underground forum, allegedly exposing enterprise business details, service metadata, and active session identifiers
- **Threat Level:** Non-ransomware breach with significant risks of unauthorized access, credential abuse, and enterprise intelligence exposure

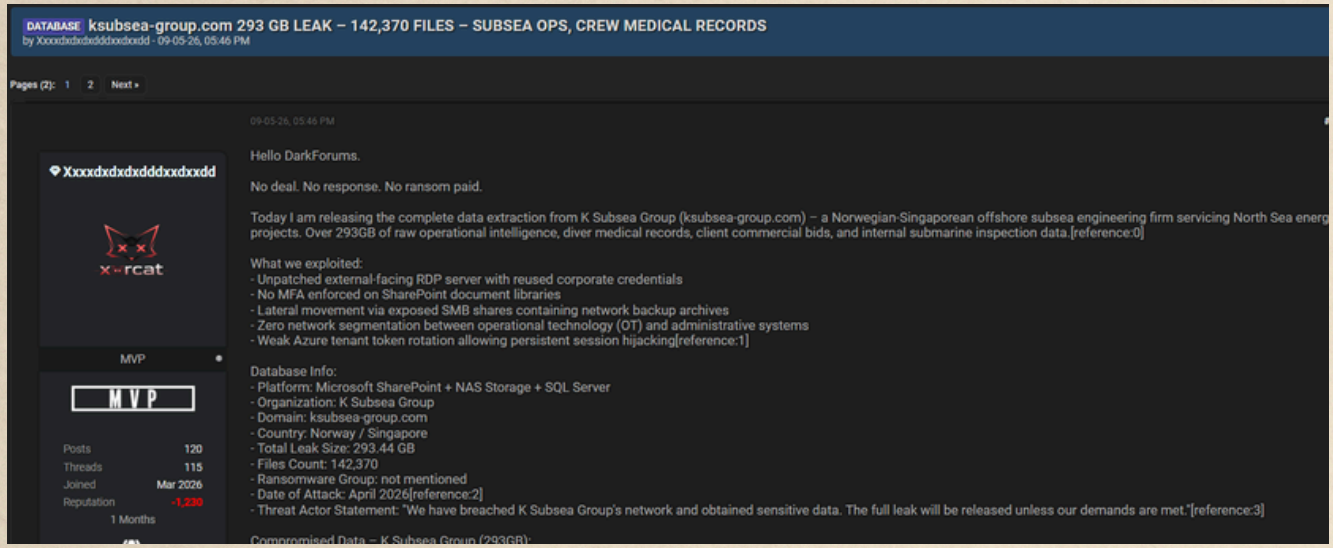
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 03 MAY - 16 MAY 2026

K Subsea Group Breach Incident

On May 09, 2026, a Singapore company K Subsea Group suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Energy / Offshore Services
Threat Actor : Xxxxdxdxdxdddxxdxxdd
Data Sold: 293 GB



Key Highlights

- **Data Exposure:** Approx 142K files (293GB) reportedly leaked, including operational data, crew medical records, and internal inspection documents
- **Threat Actor:** Linked to Xxxxdxdxdxdddxxdxxdd
- **Threat Activity :** Shared on underground forum following alleged unauthorized access to corporate infrastructure
- **Threat Level:** High-severity breach with risks to sensitive personnel data, operational security, and commercial confidentiality

GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:03 MAY - 16 MAY 2026

MBet Breach Incident

On May 12, 2026, a Brazil company MBet suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Online Gambling
Threat Actor : zSenior
Data Sold: 251 GB

Key Highlights

- **Data Exposure:** Approx 300K PII records and 200K+ KYC documents reportedly leaked, including IDs, emails, phone numbers, and personal verification data
- **Threat Actor:** Linked to zSenior
- **Threat Activity:** Shared on underground forum; exposed records include identity documents and customer account information
- **Threat Level:** Critical non-ransomware breach with high risks of identity theft, fraud, and unauthorized account misuse

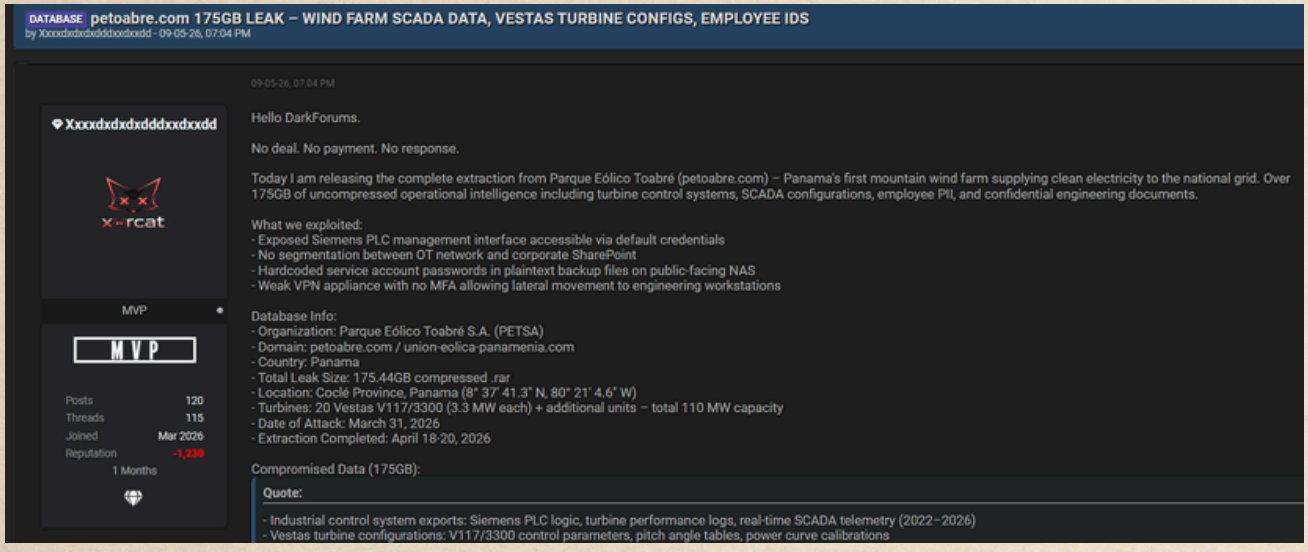
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:03 MAY - 16 MAY 2026

Parque Eólico Toabré S.A. (PETSA) Breach Incident

On May 09, 2026, a Panama company PETSA suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Energy / Renewables
Threat Actor : Xxxxdxdxdxdddxxdxxdd
Data Sold: 175 GB



Key Highlights

- **Data Exposure:** Approx 175GB of data reportedly leaked, including SCADA configurations, turbine system data, and employee identifiers
- **Threat Activity:** Shared on underground forum; alleged exposure of critical infrastructure operational documents and engineering records
- **Threat Actor:** Linked to Xxxxdxdxdxdddxxdxxdd
- **Threat Level:** Critical breach affecting energy infrastructure, with risks to operational security, employee privacy, and industrial system integrity

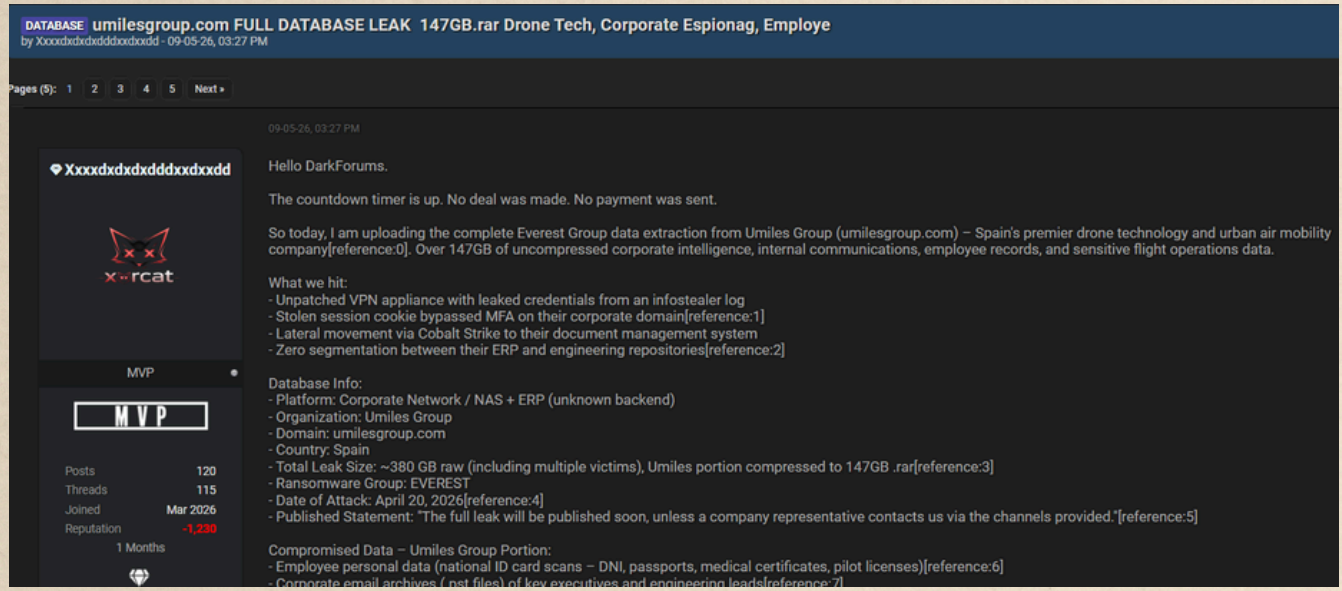
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 03 MAY - 16MAY 2026

UMILES Group Breach Incident

On May 09, 2026, a Spain company UMILES Group suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Drone Technology
Threat Actor : Xxxxdxdxdxdddxxdxxdd
Data Sold: 147 GB



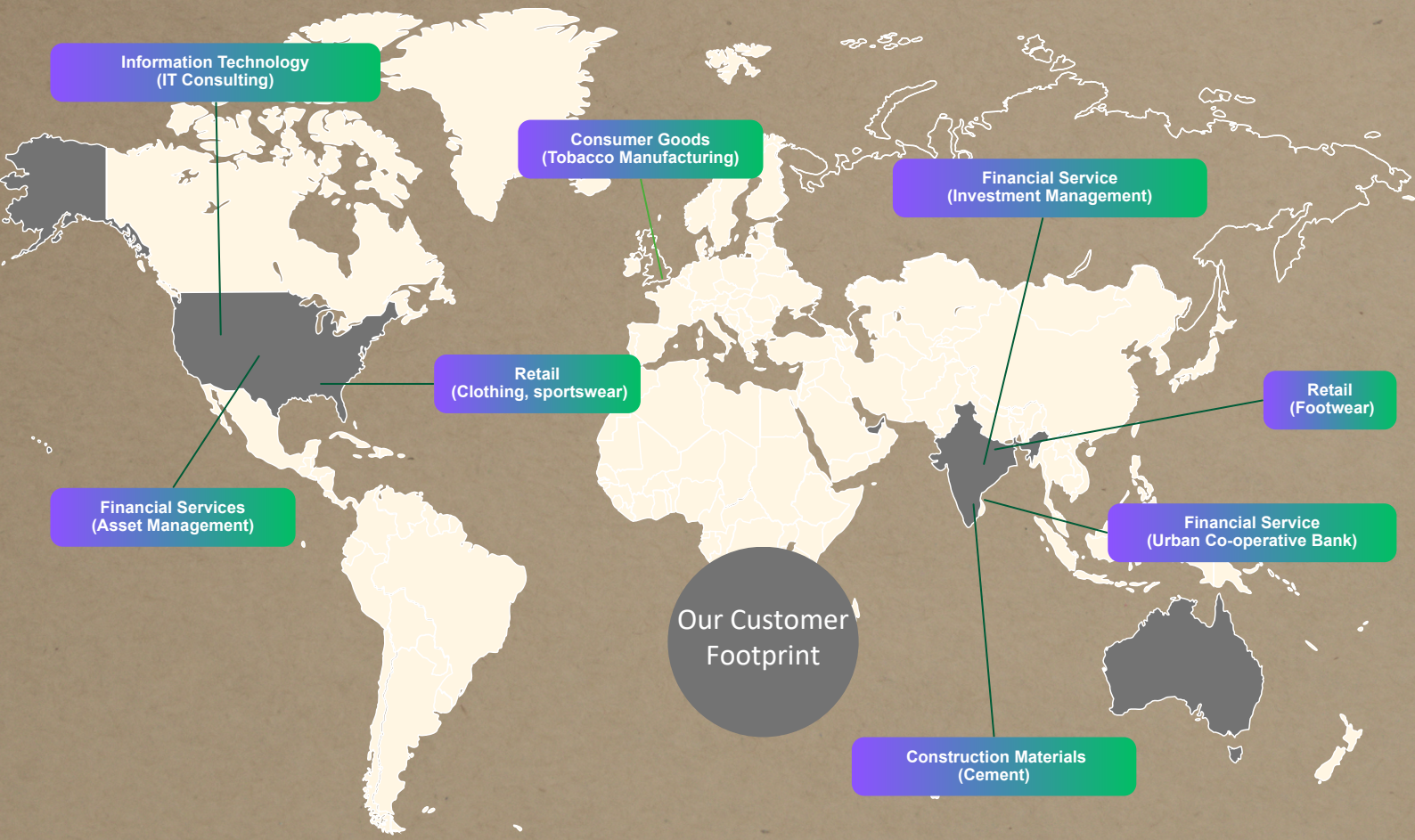
Key Highlights

- **Data Exposure:** Approx 147GB of data reportedly leaked, including employee records, internal communications, and sensitive flight operations information
- **Threat Actor:** Claimed by Xxxxdxdxdxdddxxdxxdd
- **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