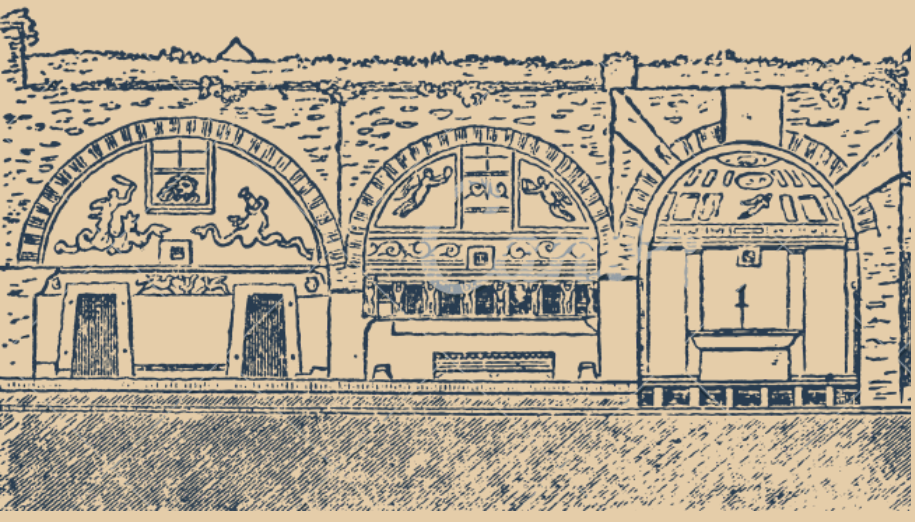
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 24 MAY – 30 MAY 2026



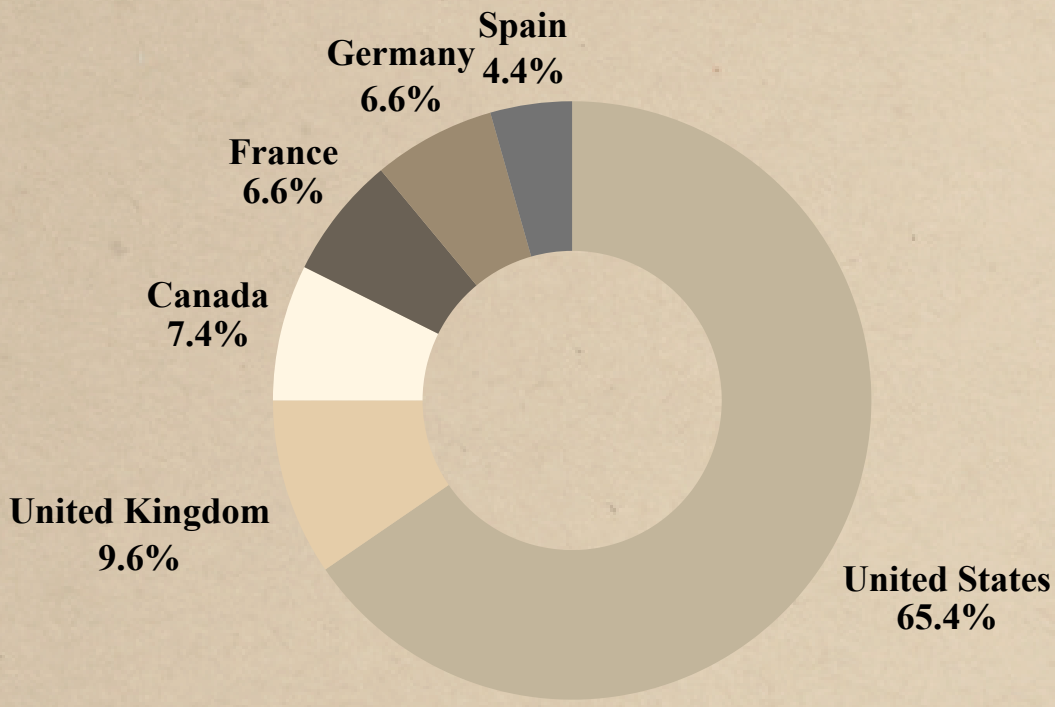
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:24 MAY - 30 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

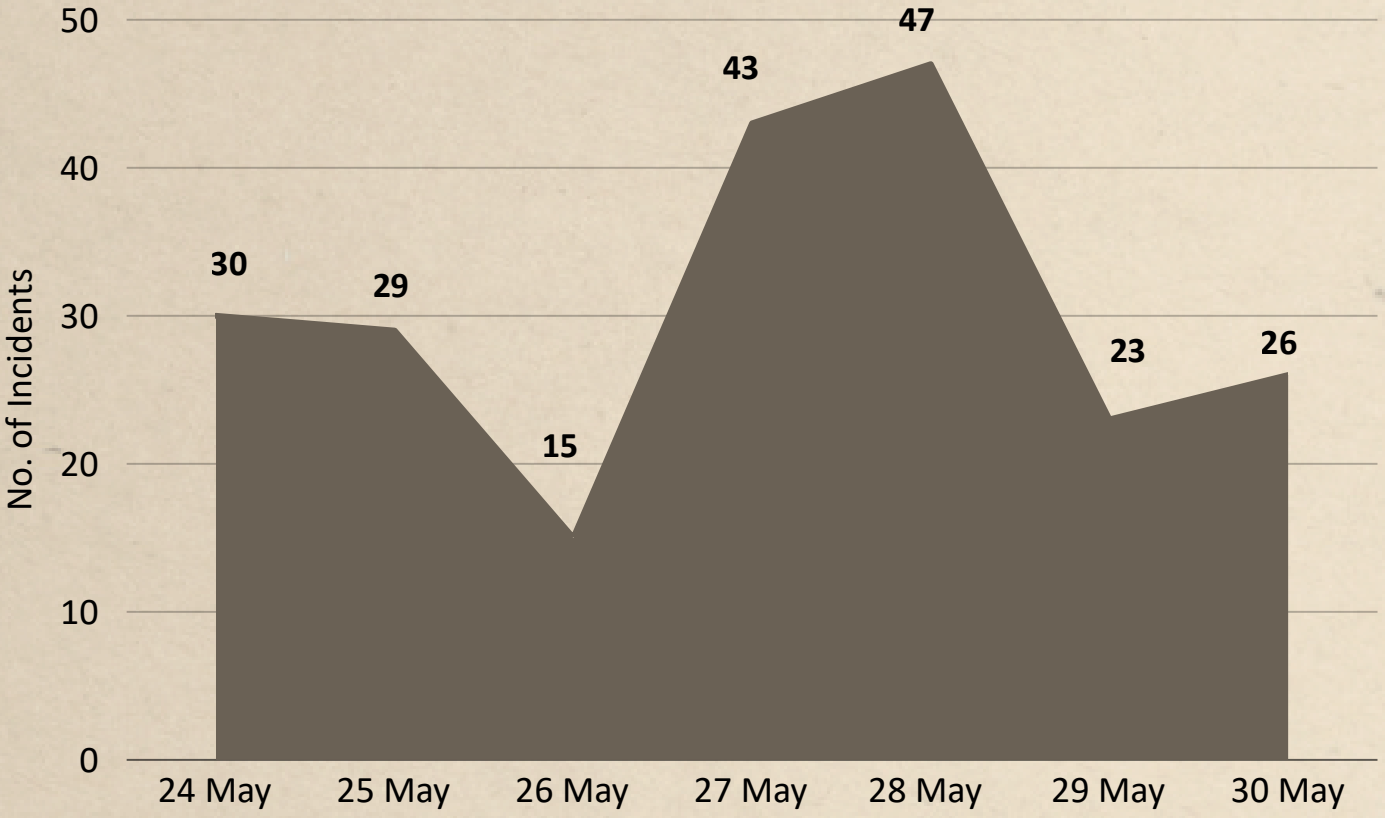
- The majority of incidents were linked to ransomware and data extortion activity, highlighting the continued dominance of financially motivated cyber threats.
- Threat groups such as **DragonForce**, **Qilin**, **The Gentlemen**, and **Akira** were most frequently observed, indicating sustained and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

Most Targeted Sector: Manufacturing
Ransomware-linked breaches: 89.7%
Total Breaches Observed: 213
Countries Affected: 46

GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD:24 MAY - 30 MAY 2026

Breach Over time

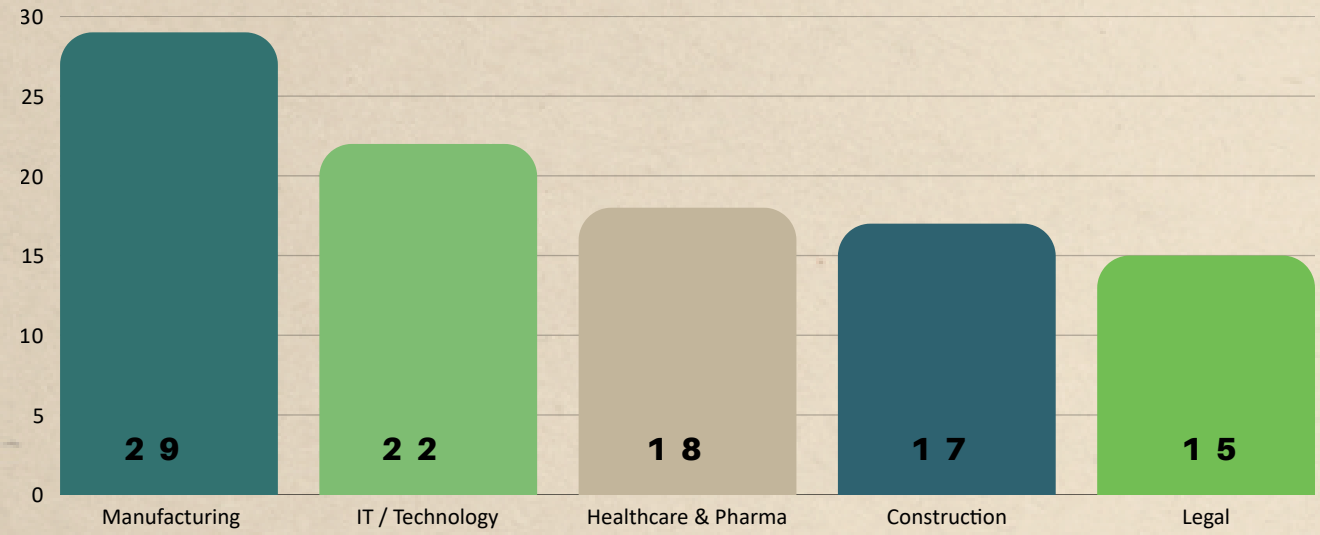


- Breach activity fluctuated throughout the period, with May 28, recording the highest spike at 47 reported incidents.
- A sharp rise was observed between May 26 and May 27, peaking at 43 incidents on May 27, indicating intensified disclosure or attack activity.
- May 26 reported the lowest number of incidents, with only 15 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: 24 MAY - 30 MAY 2026

Affected Sectors



Industry Highlights

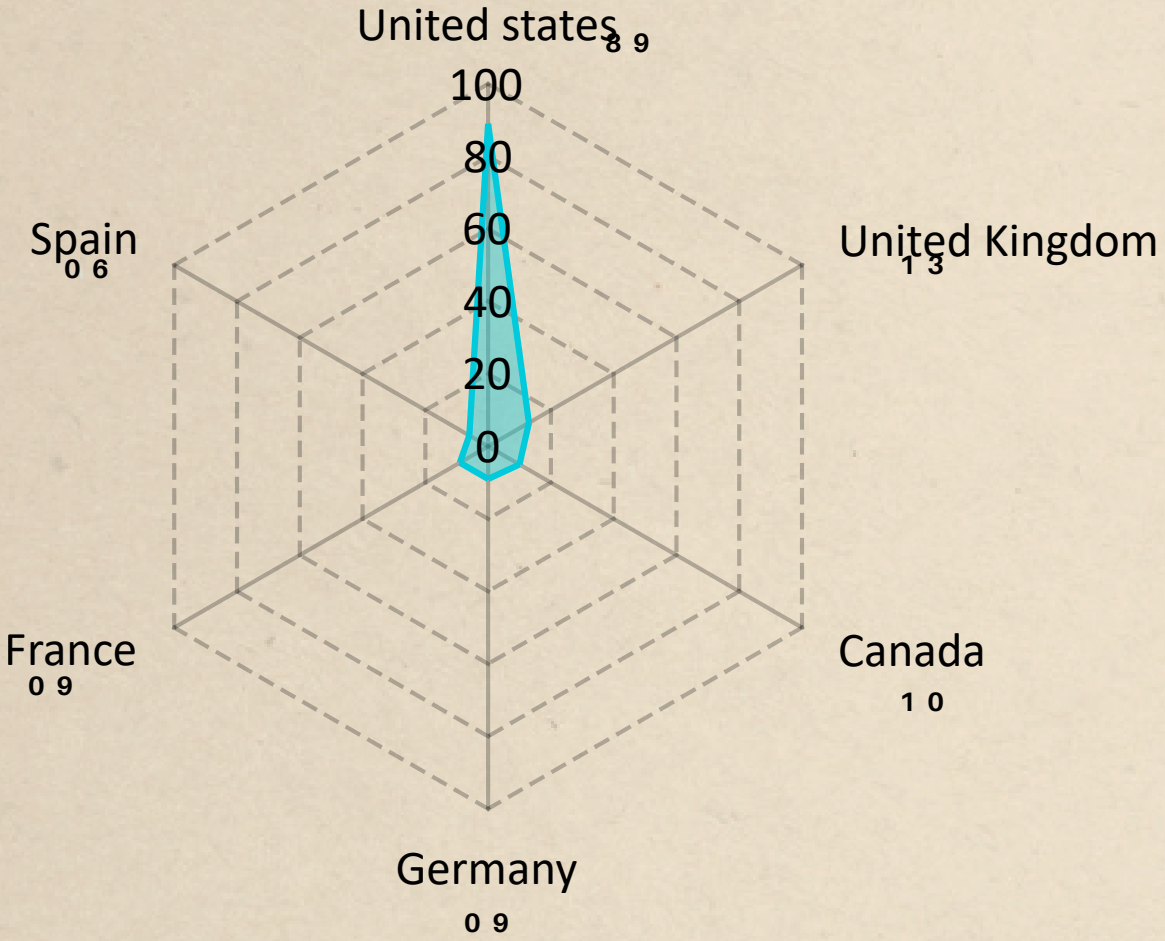
- **Manufacturing & Engineering: 29+ incidents (highest targeted sector)**
- **IT / Technology: 22+ incidents (high exposure due to digital infrastructure)**
- **Healthcare & Pharma: 18+ incidents**
- **Construction : 17+ incidents**
- **Finance / Legal / Insurance: 15+ incidents**

Industries Insight: Manufacturing and technology organizations remained the most frequently impacted, while healthcare, construction, and financial sectors continued to face significant targeting due to their critical operations, valuable data, and broad attack surfaces.

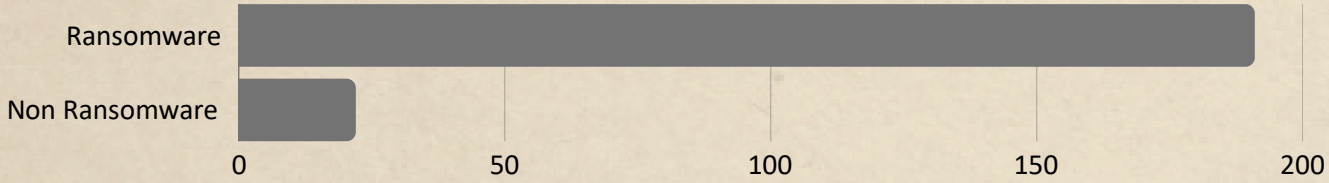
GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 24 MAY - 30 MAY 2026

Affected Countries



Actor Distribution



Ransomware dominates the threat landscape with 191+ incidents, far outpacing 22 non-ransomware cases, making it the most prevalent and impactful attack type.

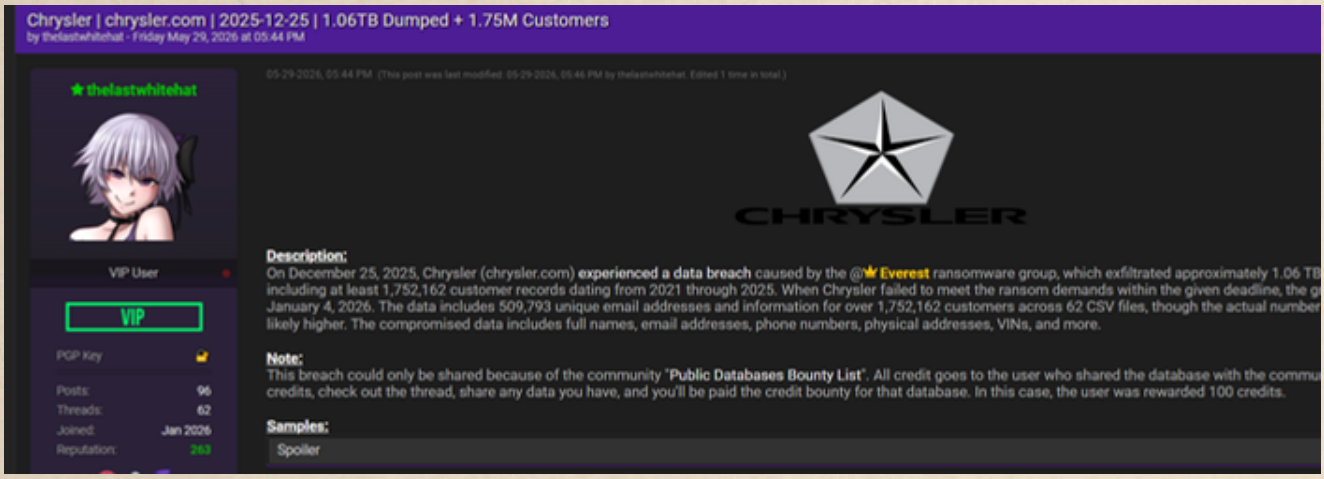
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 24 MAY - 30 MAY 2026

Chrysler Breach Incident

On May 29, 2026, a US company Chrysler suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Automotive Manufacturing
Threat Actor : Everest
Data Sold: 1.06 TB



Key Highlights

- **Data Exposure:** Approx 1.06TB of data reportedly leaked, affecting more than 1.75M customer records and containing over 509M unique email entries across 62 CSV files
- **Threat Actor:** Linked to the Everest ransomware group
- **Threat Activity:** Data allegedly released following failed ransom negotiations, exposing customer names, email addresses, phone numbers, physical addresses, VINs, and related records
- **Threat Level:** Critical ransomware-related breach with significant risks of identity theft, fraud, targeted phishing, and large-scale customer data misuse

GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 24 MAY - 30 MAY 2026

Groupe IMA Breach Incident

On May 28, 2026, a France company Groupe IMA suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Insurance & Emergency Assistance
Threat Actor : Night
Data Sold: 6.2 GB

Key Highlights

- **Data Exposure:** Approx 6.2 GB of data reportedly leaked, including medical assistance records, medical aid information, and home assistance service data
- **Threat Actor:** Linked to Night
- **Threat Activity :** Alleged exposure impacts Groupe IMA (Inter Mutuelles Assistance), a provider of insurance and mutual assistance services
- **Threat Level:** High-risk breach involving potentially sensitive personal and assistance-related information, with risks of privacy violations, fraud, and unauthorized access to customer data

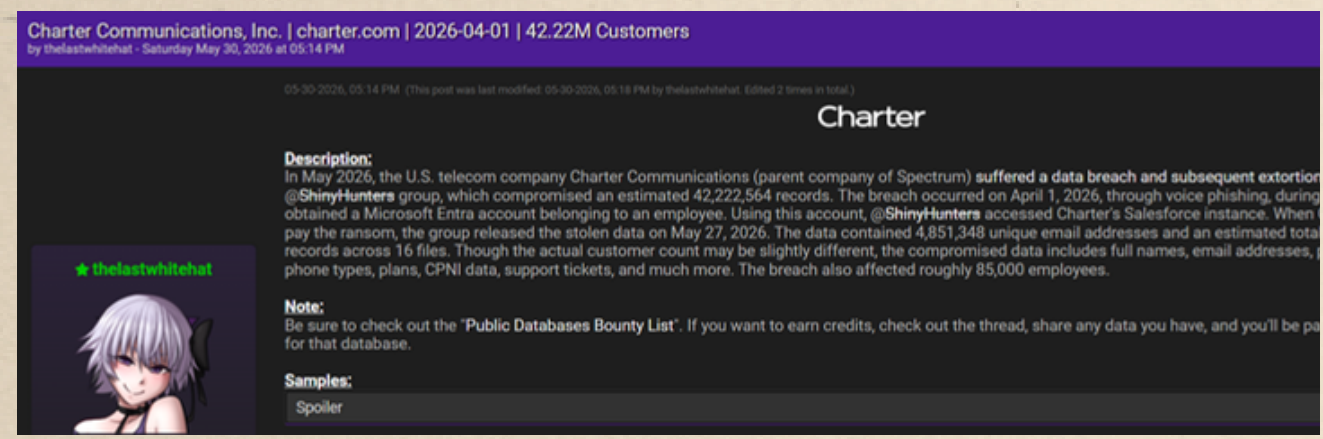
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:24 MAY - 30 MAY 2026

Charter Communications, Inc Breach Incident

On May 30, 2026, a USA company Charter Communications, Inc suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Telecommunications
Threat Actor : ShinyHunters
Data Sold: 1.5 GB



Key Highlights

- **Data Exposure:** Approx 42.22M customer records reportedly leaked, including names, email addresses, phone numbers, account details, support tickets, and CPNI-related data
- **Threat Actor:** Linked to ShinyHunters
- **Threat Activity:** Data allegedly released following a voice-phishing attack and subsequent extortion attempt targeting Charter's Salesforce environment
- **Threat Level:** Critical breach with risks of identity theft, targeted phishing, account fraud, and exposure of sensitive telecommunications customer information

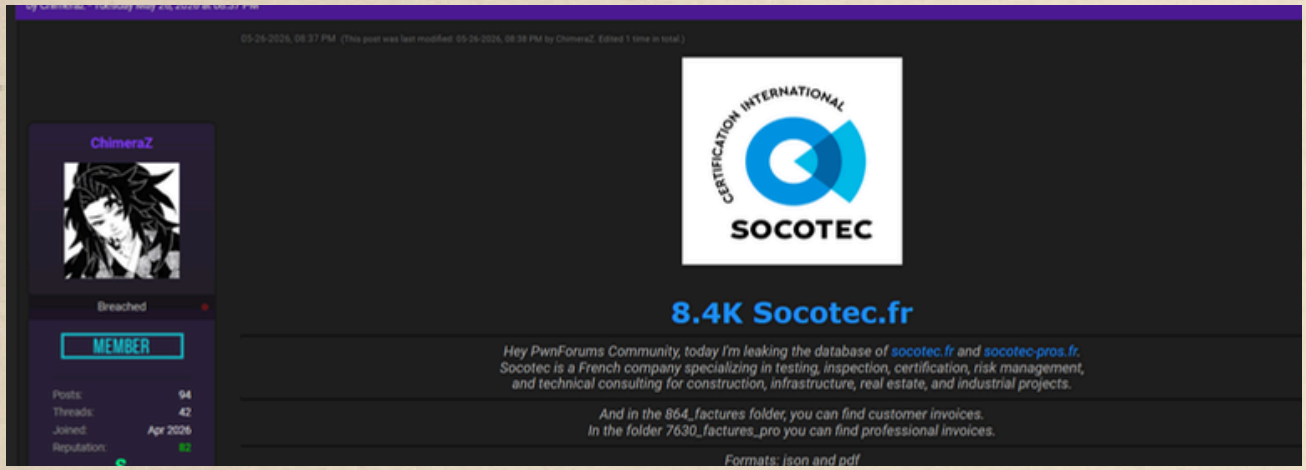
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:24 MAY - 30 MAY 2026

SOCOTEC France Breach Incident

On May 26, 2026, a France company SOCOTEC France suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Business Services / Risk Management
Threat Actor :ChimeraZ
Data Sold: 990 MB



Key Highlights

- **Data Exposure:** Approx 8.4K records reportedly leaked from Socotec.fr and Socotec-Pros.fr, including customer and professional invoice data
- **Threat Activity:** Shared on underground forum; exposed files allegedly include JSON and PDF documents containing business-related information
- **Threat Actor:** Linked to ChimeraZ
- **Threat Level:** Non-ransomware breach with risks of unauthorized access, business data exposure, invoice fraud, and reputational impact

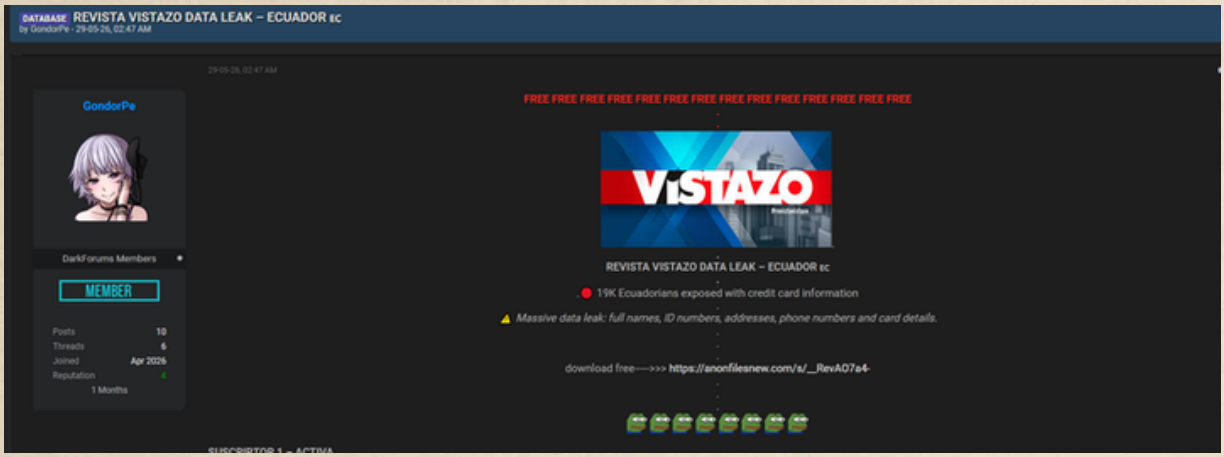
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 24 MAY - 30MAY 2026

Revista Vistazo Breach Incident

On May 29, 2026, a Ecuador company Revista Vistazo suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Media & Publishing / News Journalism
Threat Actor : GondorPe
Data Sold: 188 MB



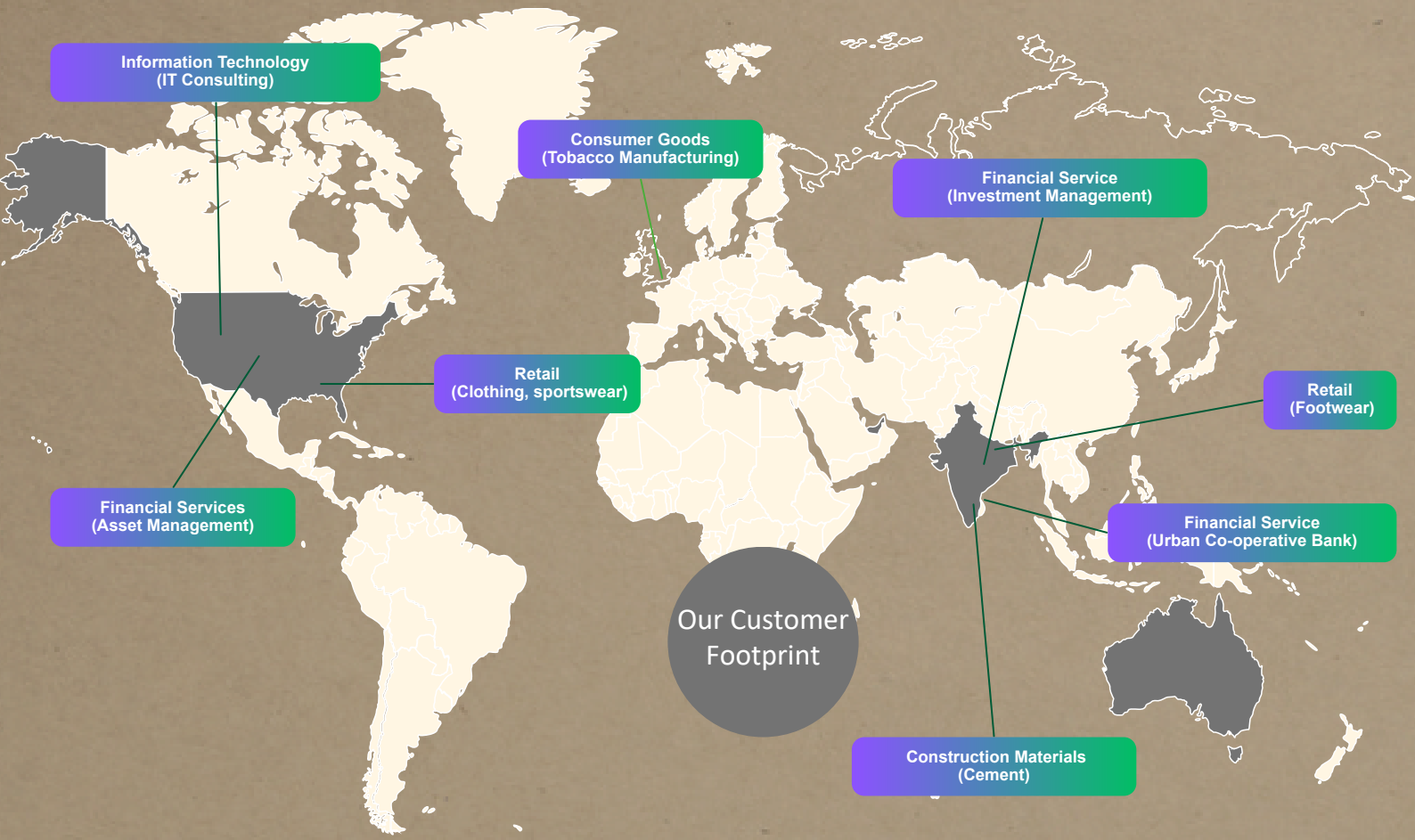
Key Highlights

- **Data Exposure:** Approx 19K records reportedly leaked, including full names, ID numbers, addresses, phone numbers, and payment card-related information
- **Threat Actor:** Linked to GondorPe
- **Threat Activity:** Shared on underground forum with publicly accessible download links and sample data references
- **Threat Level:** High-risk data exposure with potential for identity theft, financial fraud, phishing attacks, and unauthorized use of personal information

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