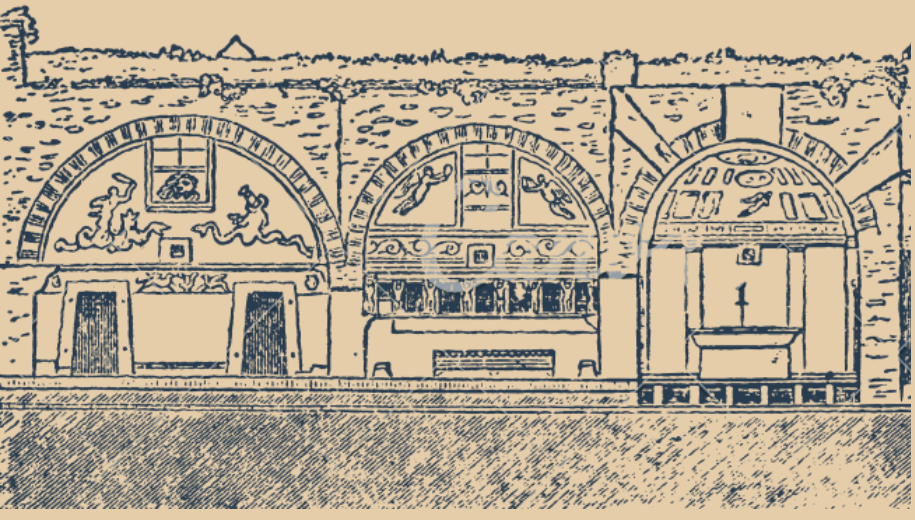
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 28 JUNE – 04 JULY 2026



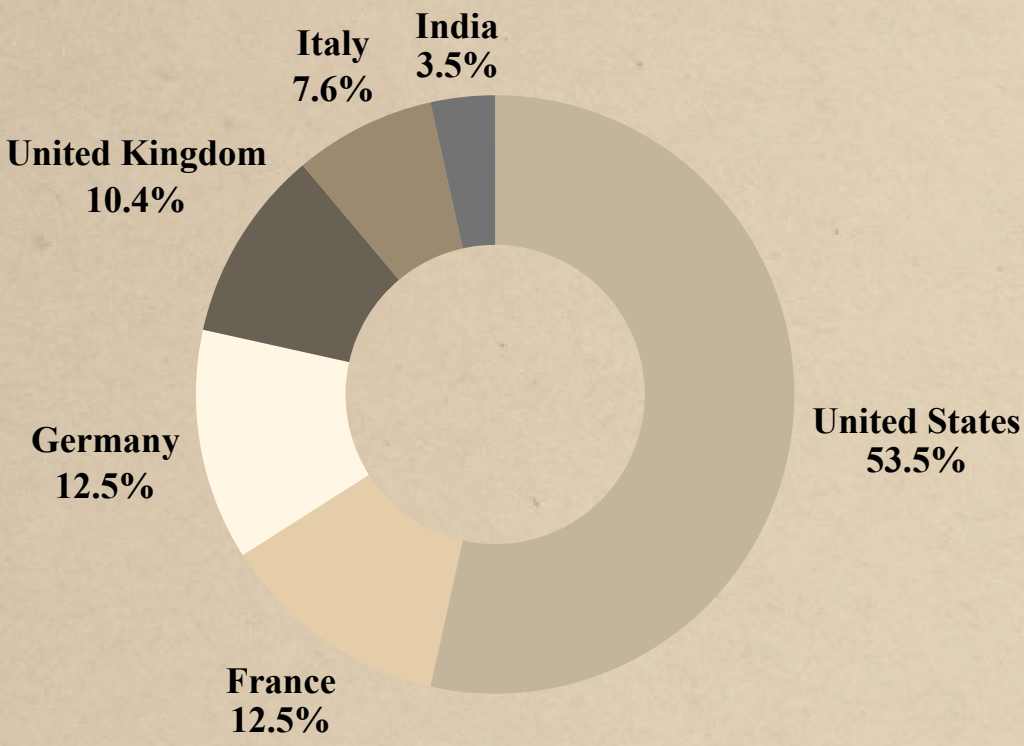
GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 28 JUNE - 04 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 **The Gentlemen**, **Qilin**, **IncRansom**, and **Settra** were most frequently observed, indicating sustained and coordinated attack campaigns.

Most Targeted Sector: Manufacturing

Total Breaches Observed: 256

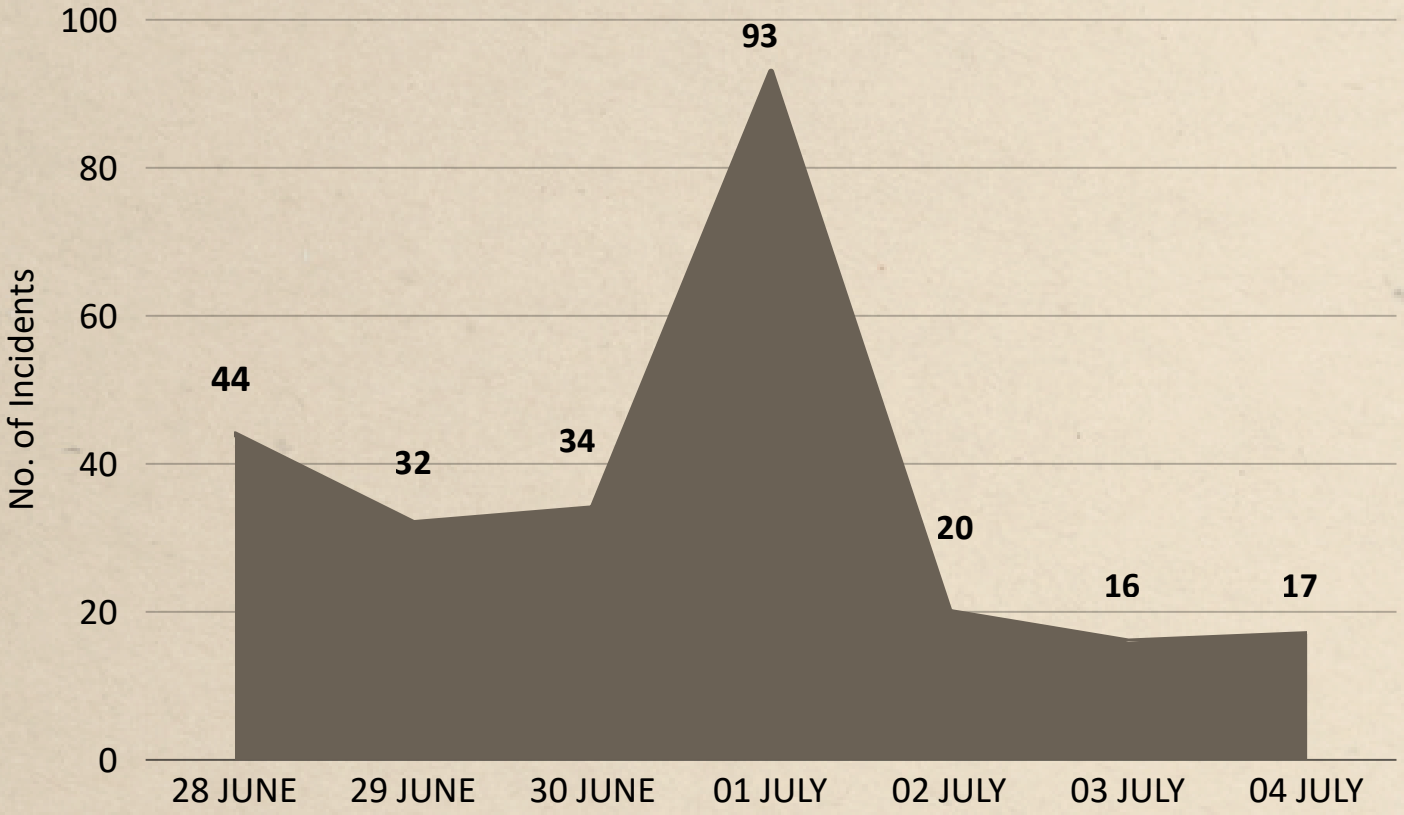
Ransomware-linked breaches: 80.1%

Countries Affected: 51

GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 28 JUNE - 04 JULY 2026

Breach Over time

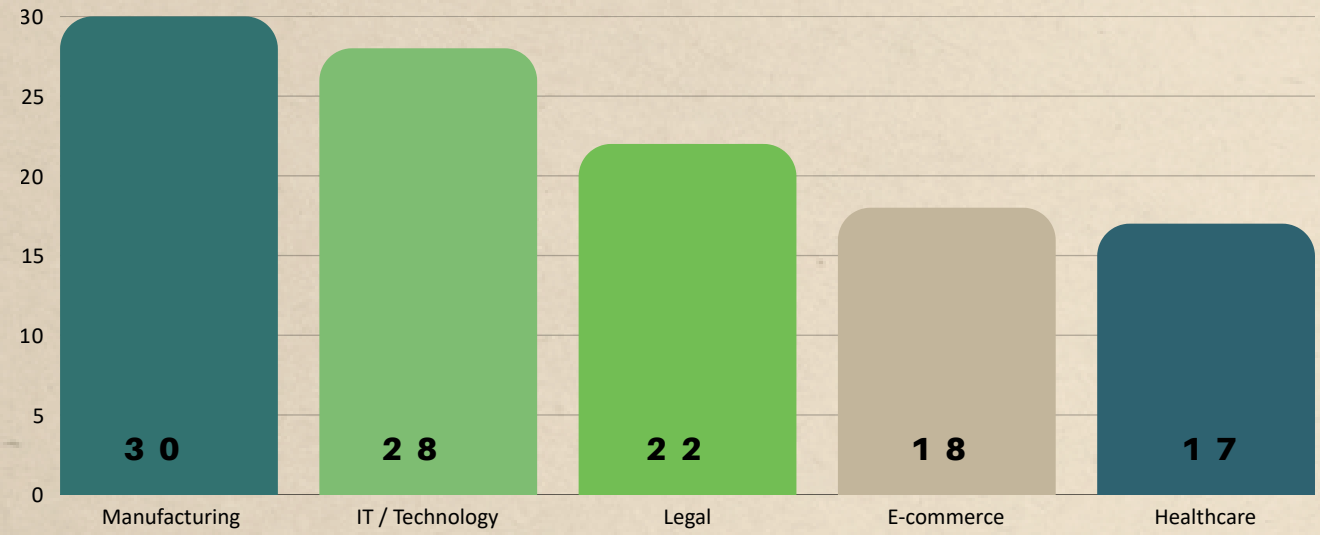


- Breach activity fluctuated throughout the period, with July 01, recording the highest spike at 93 reported incidents.
- A sharp rise was observed between June 30 and June 28, peaking at 44 incidents on June 28, indicating intensified disclosure or attack activity.
- July 03 reported the lowest number of incidents, with only 16 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:28JUNE-04JULY 2026

Affected Sectors



Industry Highlights

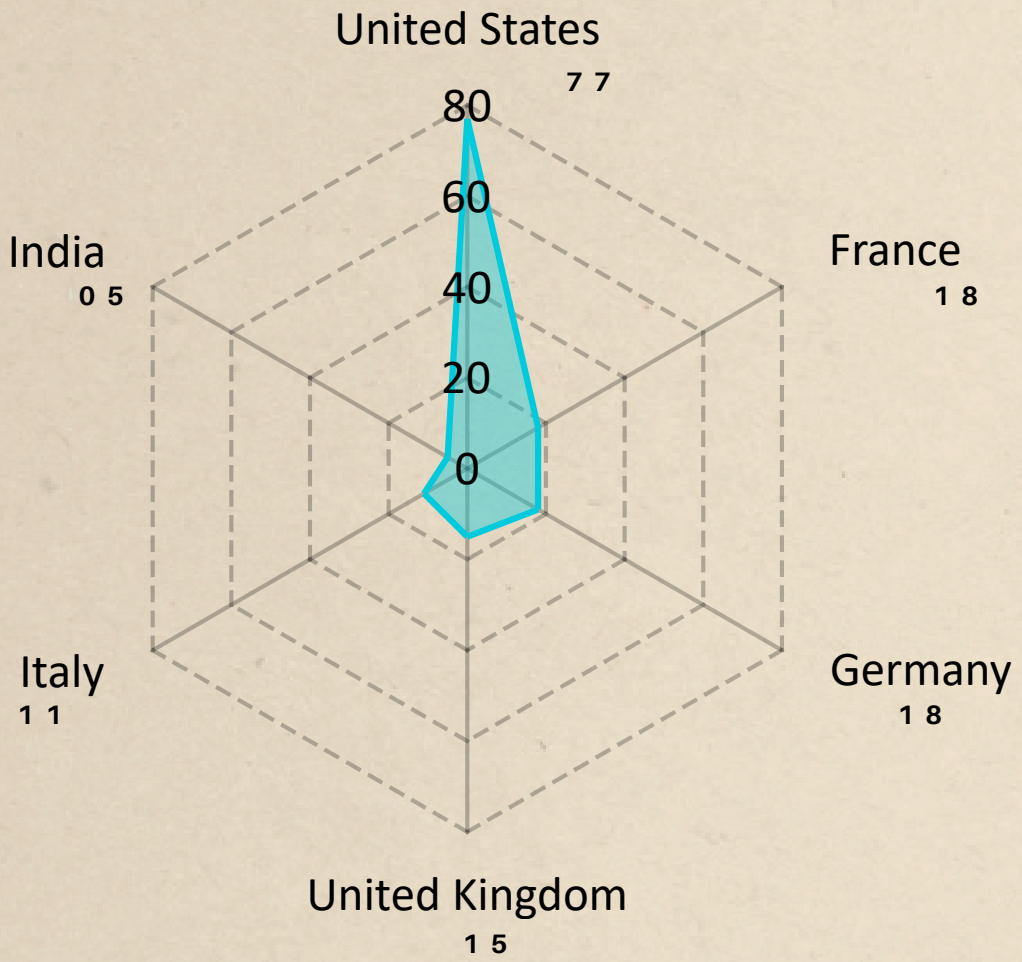
- **Manufacturing & Engineering: 30+ incidents (highest targeted sector)**
- **IT / Technology: 28+ incidents (high exposure due to digital infrastructure)**
- **Legal : 22+ incidents**
- **E-Commerce : 18+ incidents**
- **Healthcare : 17+ incidents**

Industries Insight: Manufacturing and technology remained the primary targets for threat actors, followed by finance, retail, and healthcare. These sectors continue to face elevated risk due to their reliance on digital infrastructure, extensive customer data, and business-critical operations.

GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 28 JUNE - 04 JULY 2026

Affected Countries



Actor Distribution

Ransomware dominates the threat landscape with 205+ incidents, far outpacing 51 non-ransomware cases, making it the most prevalent and impactful attack type.

GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:28JUNE-04JULY 2026

CTM India Limited motherson INDIA Breach Incident

On July 01, 2026, **CTM India Limited motherson INDIA,** a finance company suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector : Finance
Threat Group (Ransomware) : thegentlemen
Data Sold: 83 bytes
Country: India

Key Highlights

- **Data Exposure:** Alleged CIM India Limited (Motherson India) contact-related data was listed on a cybercrime leak site.
- **Threat Group:** Linked to **The Gentlemen**
- **Source & Risk:** A file named CONTACT_BUY_DATA.txt was published, indicating the availability of alleged contact data for sale or distribution.
- **Threat Activity:** Public listing of alleged corporate data on a cybercrime platform, suggesting unauthorized access and potential commercialization.
- **Threat Level:** Medium due to the limited visible data, though the listing may indicate broader unauthorized access or attempted data sale

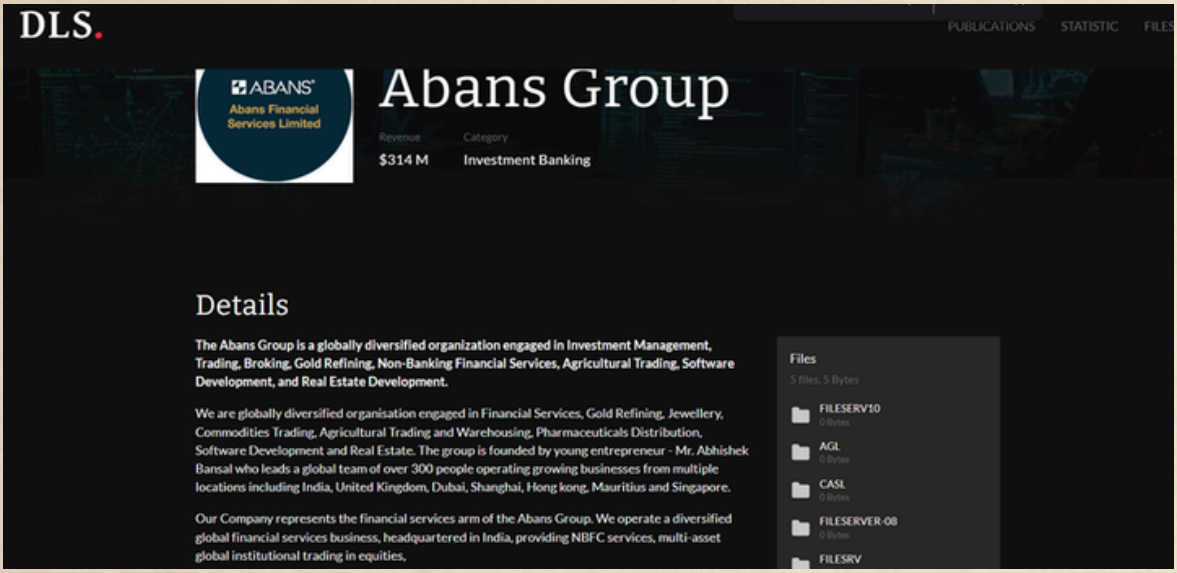
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:28JUNE-04JULY 2026

Abans Finserv Breach Incident

On June 29, 2026, **Abans Finserv,** a finance company suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Financial Services
Threat Group (Ransomware) : Blacknevas
Data Sold : Unknown
Country: India



Key Highlights

- **Data Exposure:** Abans Group was listed on a data leak site, indicating an alleged compromise of corporate data.
- **Threat Group :** Posted by **Blacknevas**
- **Source & Risk:** The listing references multiple internal file repositories, suggesting potential exposure of organizational data and systems..
- **Threat Activity :** Public listing of an alleged victim on a data leak site as part of a data extortion campaign.
- **Threat Level:** High due to the potential exposure of sensitive corporate information and internal business assets.

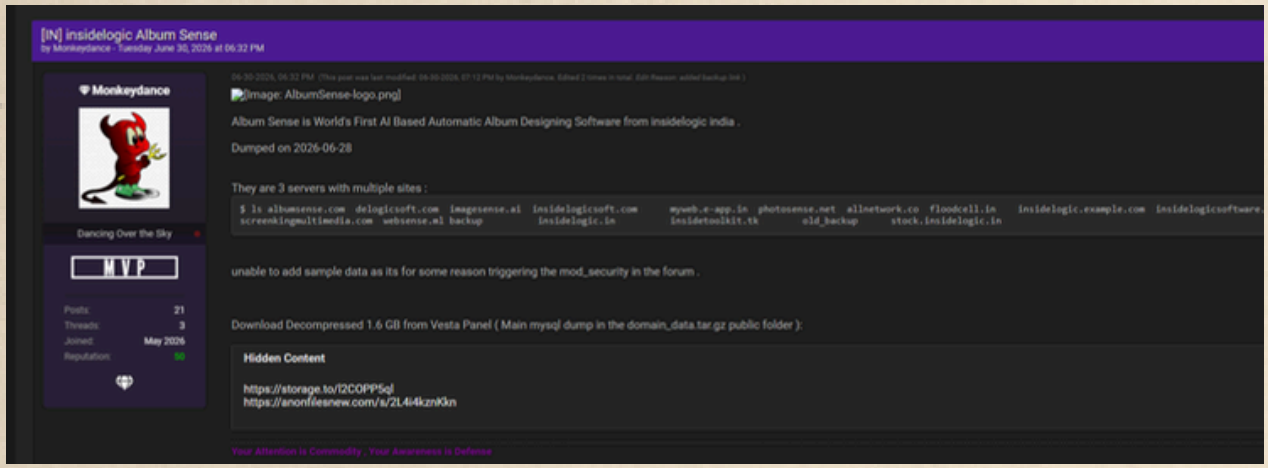
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD: 28 JUNE - 04 JULY 2026

InsideLogic Software Pvt. Ltd. Breach Incident

On June 30, 2026, **InsideLogic Software Pvt. Ltd**., software company suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Software Development
Threat Group (Ransomware) : Monkeydance
Data Sold : 1.6 GB
Country : India



Key Highlights

- **Data Exposure:** Alleged 1.6 GB database and server data associated with InsideLogic (Album Sense) was published on a cybercrime forum.
- **Threat Actor:** Linked to **Monkeydance**
- **Source & Risk:** The post claims data was extracted from multiple servers, including Vesta Panel backups and MySQL database dumps, with download links provided.
- **Threat Activity:** Public disclosure and distribution of alleged stolen corporate data as part of a data extortion campaign.
- **Threat Level:** High due to the potential exposure of databases, server backups, and sensitive business information.

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:28JUNE-04JULY 2026

Hanjoong NCS Co., Ltd. Breach Incident

On July 04, 2026, **Hanjoong NCS Co., Ltd,** a Manufacturing company, suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector : Manufacturing
Threat Actor : Moneyistime
Data Sold: 463 GB
Country : South Korea

Key Highlights

- **Data Exposure:** Alleged 460 GB database of Hanjoong NCS Co., Ltd. was advertised for sale on a cybercrime forum.
- **Threat Activity:** Sale of alleged stolen corporate data on a cybercrime marketplace, indicating data theft and monetization.
- **Threat Actor:** Linked to **Moneyistime**
- **Source & Risk:** The post claims to include ERP backups, HRM data, Oracle databases, and other corporate backups, with preview links provided.
- **Threat Level:** Critical due to the large volume of data and the alleged exposure of enterprise backups, HR records, ERP systems, and databases.

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:28JUNE-04JULY 2026

ArthurPro.fr Breach Incident

On July 01, 2026, **ArthurPro.fr ,** a real estate company suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Real Estate Tech
Threat Actor : ChimeraZ
Data Sold: 1.85 GB
Country : France

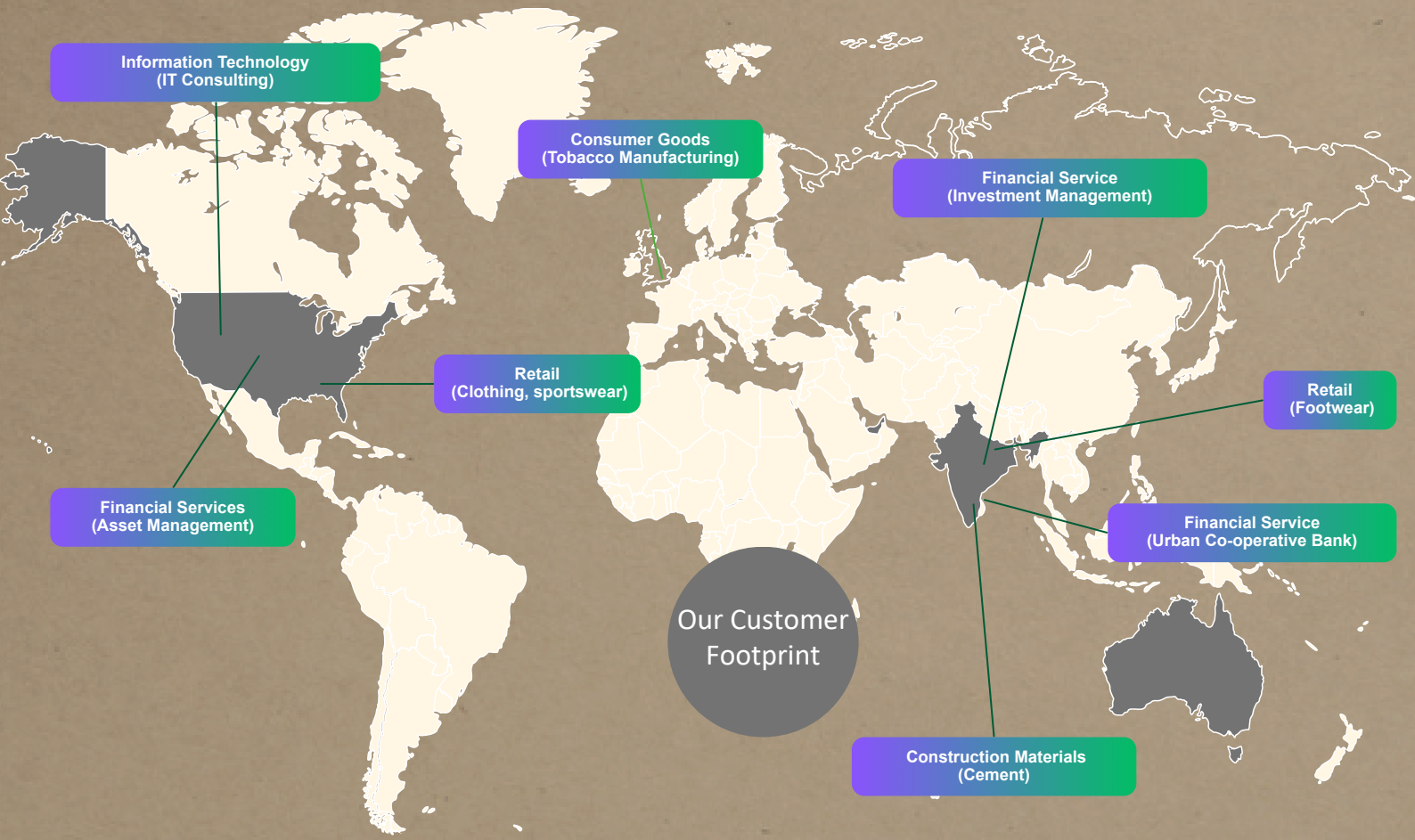
Key Highlights

- **Data Exposure:** Alleged 2.20 GB database from ArthurPro.fr was published on a cybercrime forum.
- **Threat Actor:** Linked to **ChimeraZ**
- **Source & Risk:** The leaked archive reportedly contains 817 files related to ArthurPro.fr, with download links shared publicly.
- **Threat Activity:** Public disclosure of alleged stolen corporate data as part of a data leak campaign.
- **Threat Level:** High due to the potential exposure of business data and confidential organizational 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