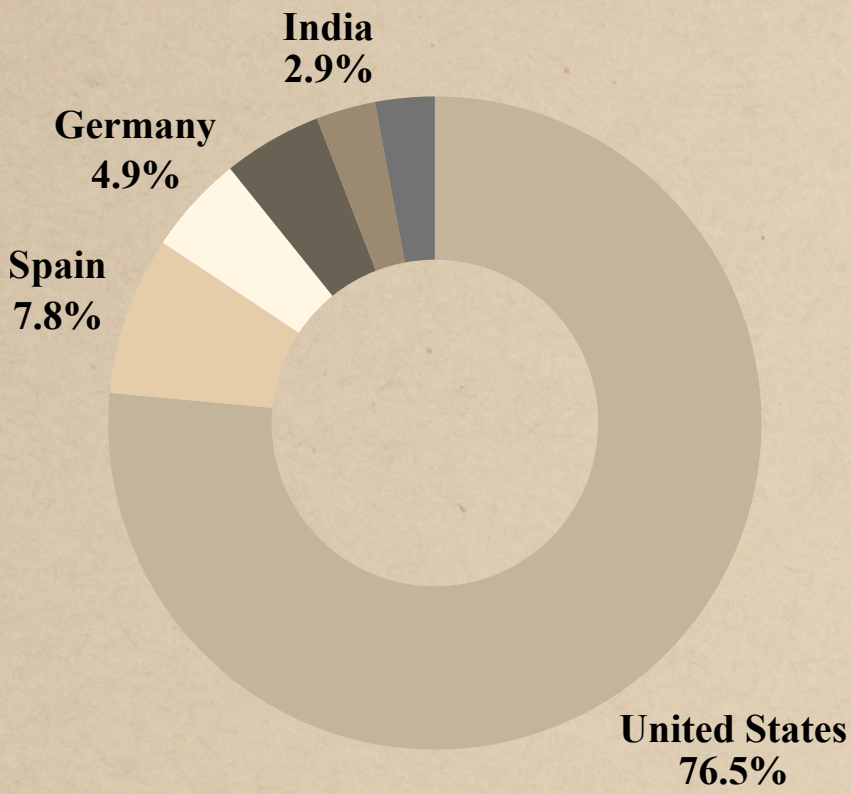
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 12 APR - 18 APR 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 ransomware-driven, highlighting continued reliance on extortion-based attack models.
- hreat groups such as coinbase cartel, dragonforce, and shinyhunters were repeatedly observed, indicating ongoing coordinated campaigns.

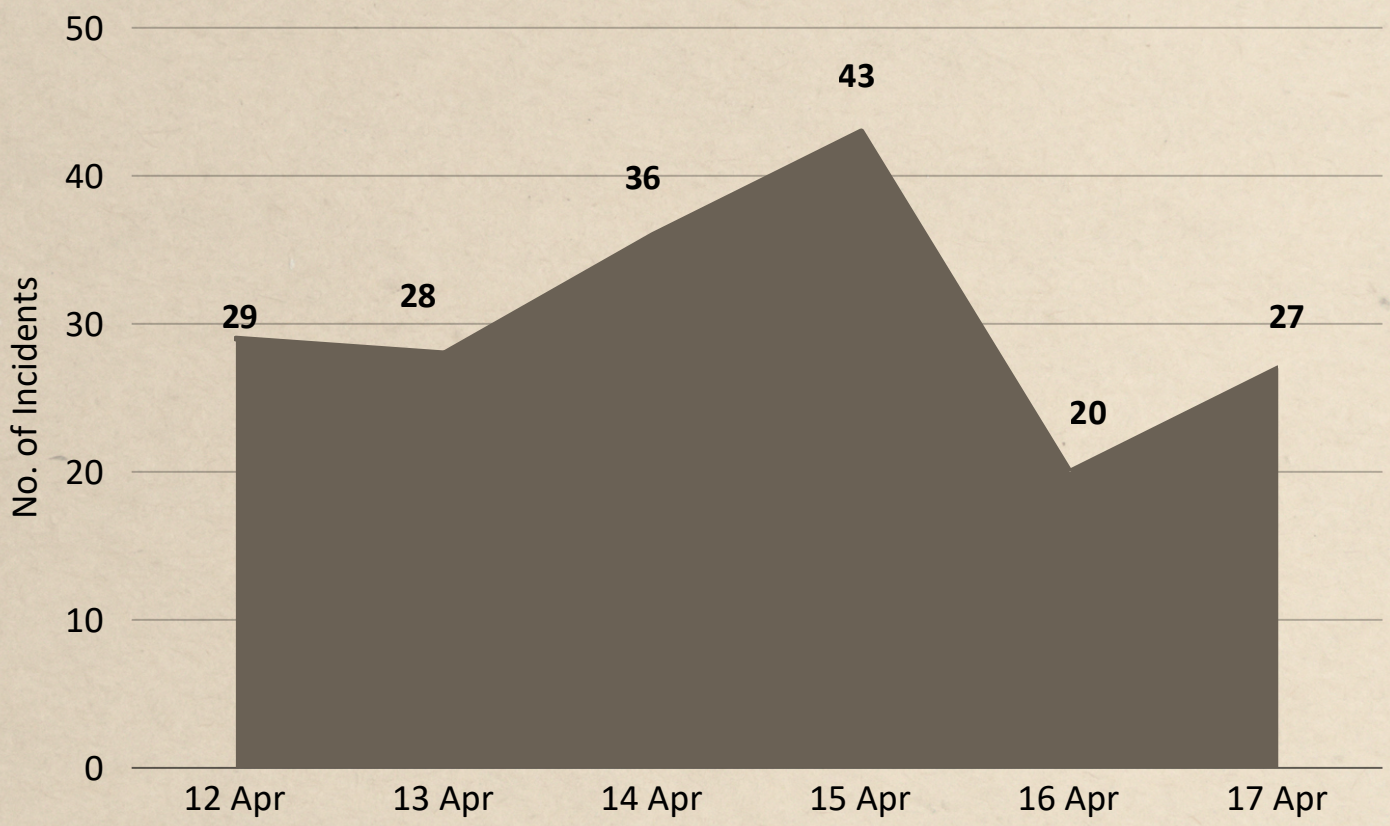
Most Targeted Sector: IT/ Technology
Ransomware-linked breaches: 93.4%

Total Breaches Observed: 196
Countries Affected: 45

GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 12 APR - 18 APR 2026

Breach Over time

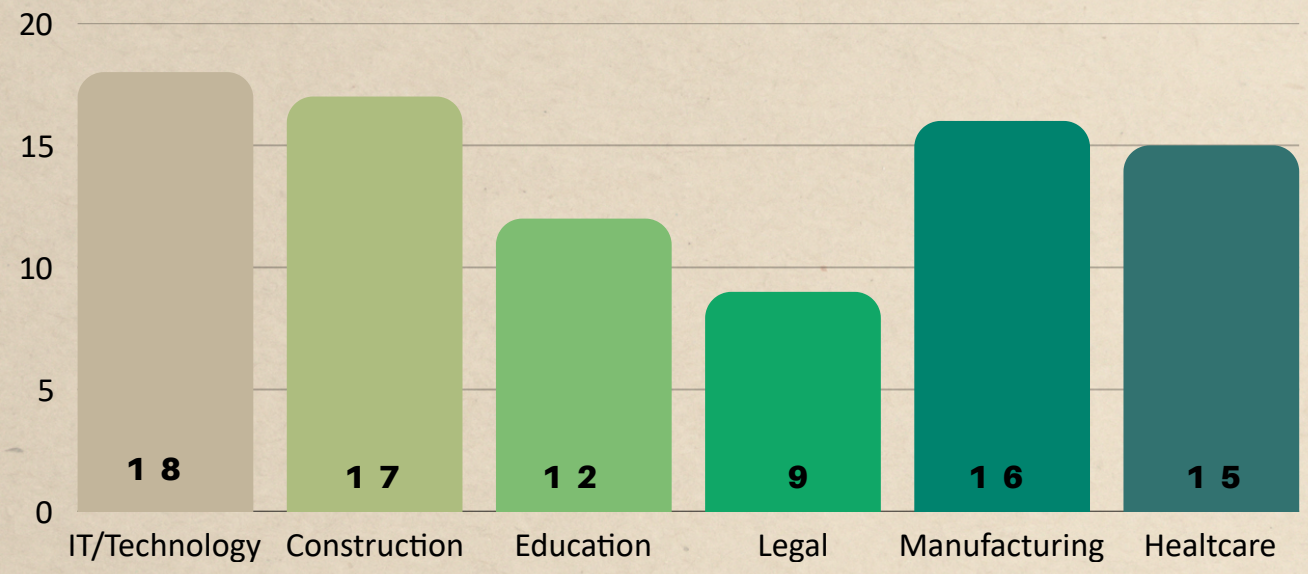


- Breaches saw a steady climb this week, with April 15 recording the most at 43 incidents.
- Activity rose April 12–15, dropped sharply on April 16 and rebounded slightly April 17, suggesting possible coordinated disclosures.
- April 16 saw the fewest incidents, with 20 reported.
- Overall, the trend reflects a mid-week surge followed by a brief decline and stabilization.

GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 12 AAPR - 18 APR 2026

Affected Sectors



Industry Highlights

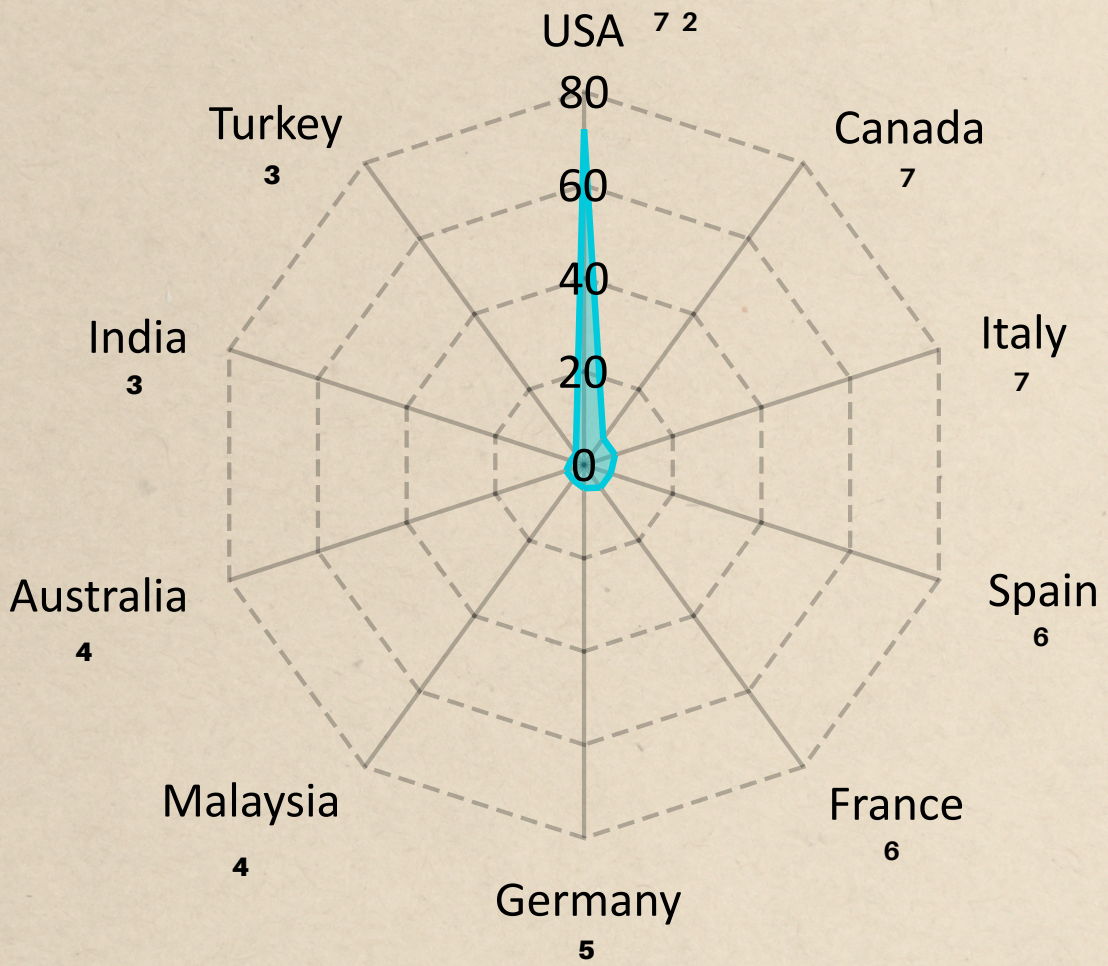
- **IT/Technology: 18** (Highest Incidents)
- **Construction: 17 incidents**
- **Manufacturing: 16 incidents**
- **Healthcare: 15 incidents (notable activity in critical services)**
- **Education: 12 incidents**
- **Legal: 9 incidents (lower reported activity)**

Industries Insight: Infrastructure-driven and data-intensive sectors remain primary targets for threat actors

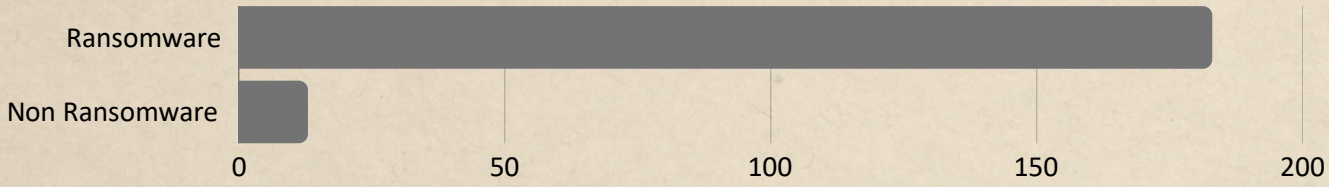
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 12 APR - 18 APR 2026

Affected Countries



Actor Distribution



Ransomware dominates the threat landscape with 180+ incidents, far outpacing 13 non-ransomware cases, making it the most prevalent and impactful attack type.

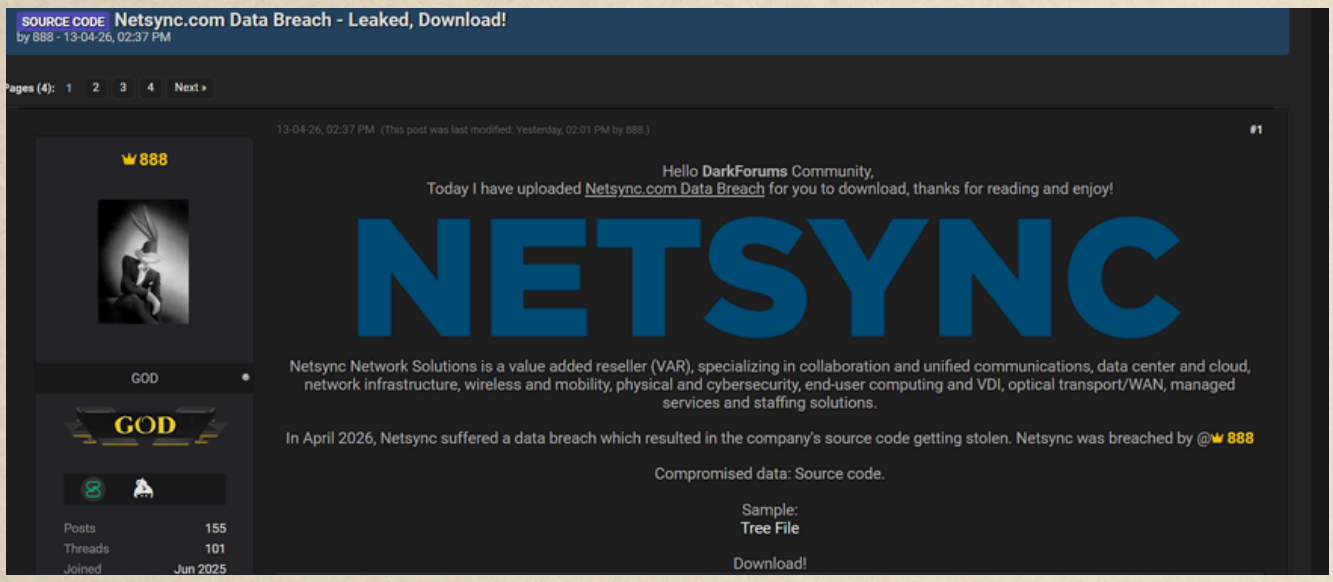
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 12 APR - 18 APR 2026

Netsync Breach Incident

On April 13, 2026, a US company Netsync (Netsync Network Solutions), suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Technology
Threat Actor : 888
Data Sold: 8.7 Gb



Key Highlights

- **Data Exposure:** Leaked dataset includes source code and sensitive internal
- **Data Impact:** Potential risk to organization's infrastructure and client environments
- **Source & Risk:** Shared on a hidden underground forum, suggesting controlled access and possible monetization
- **Threat Level:** Non-ransomware breach, but source code exposure increases risk of exploitation, unauthorized access, and supply chain attacks

GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 12 APR - 18 APR 2026

Insei Breach Incident

On April 12, 2026, INSEI experienced a notable data exposure affecting a public-sector entity and sensitive information.

Company Sector: **Government**
Threat Actor : **ChimeraZ**
Data Sold: **448 Mb**

Key Highlights

- **Data Exposure:** Approx 2.7K records leaked, potentially containing sensitive institutional or user data
- **Source & Risk:** Shared on hidden underground forum; possible monetization
- **Threat Actor:** Linked to ChimeraZ
- **Threat Level:** Non-ransomware breach with risks of unauthorized access, misuse, and reputational impact

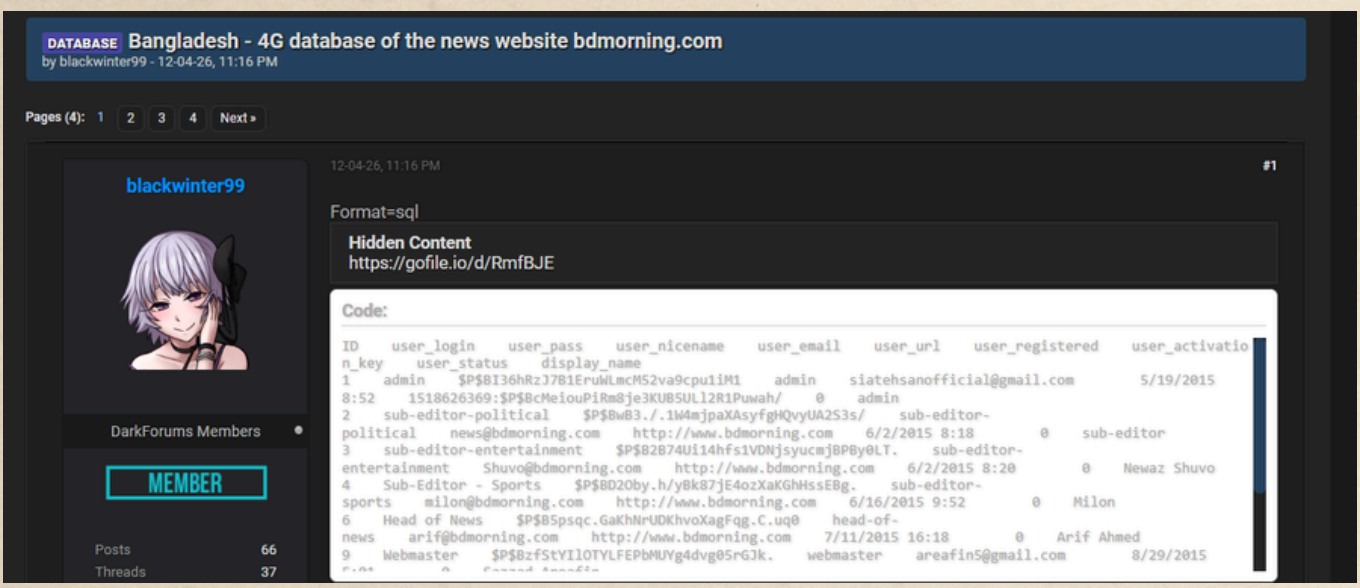
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 12 APR - 18 APR 2026

BDMorning Breach Incident

April 12, 2026 - BDMorning News, a Bangladesh-based organization in the Media / Online News Portal sector, experienced a notable data exposure affecting media operations and sensitive database information.

Company Sector: Media
Threat Actor : blackwinter99
Data Sold: 299 Mb



Key Highlights

- **Data Exposure:** Database info leaked, potentially including CMS and user data
- **Source & Risk:** Shared on hidden underground forum; possible monetization
- **Threat Actor:** Linked to blackwinter99
- **Threat Level:** Non-ransomware breach with risks of unauthorized access, misuse, and disruption to media operations and information integrity

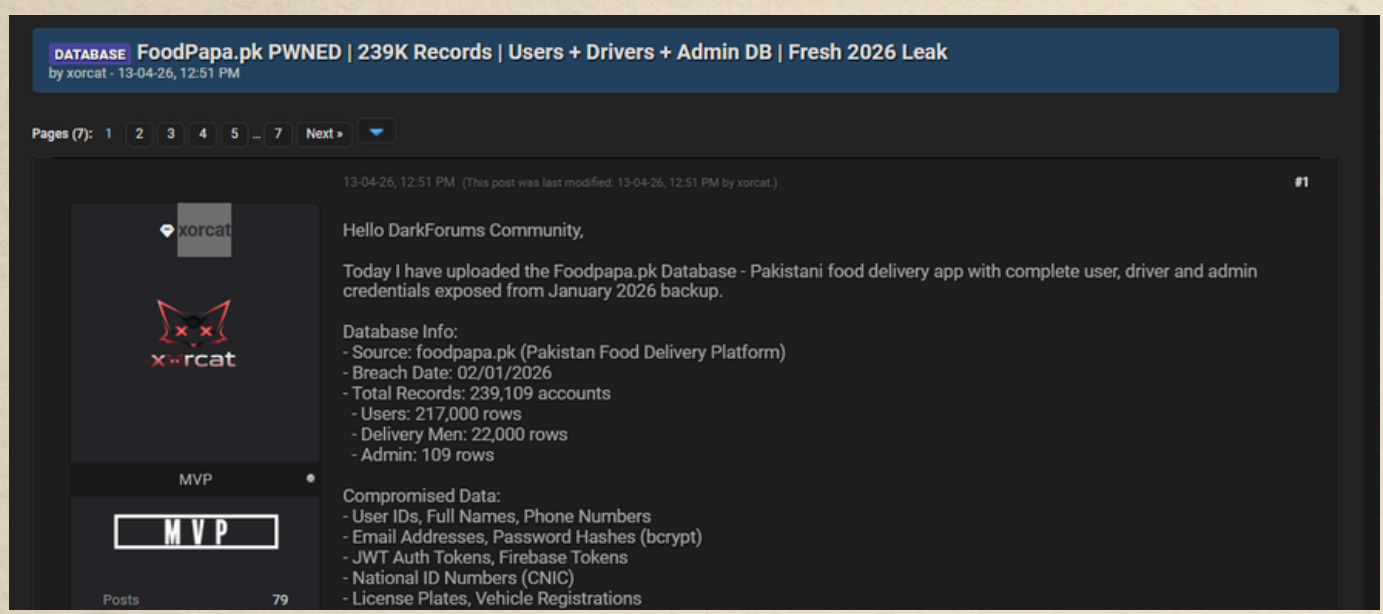
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 12 APR - 18 APR 2026

FoodPapa Breach Incident

FoodPapa a Pakistan-based organization in the Retail / E-commerce sector, suffered a data exposure on April 13, 2026, impacting customer, driver, and administrative records.

Company Sector: Retail
Threat Actor : xorcat
Data Sold: 250 Mb



Key Highlights

Data Exposure: Approx 239K records leaked, including user, driver, and admin data
Source & Risk: Shared on hidden underground forum; possible monetization
Threat Actor: Linked to xorcat
Threat Level: Non-ransomware breach with risks of data misuse, unauthorized access, and operational impact

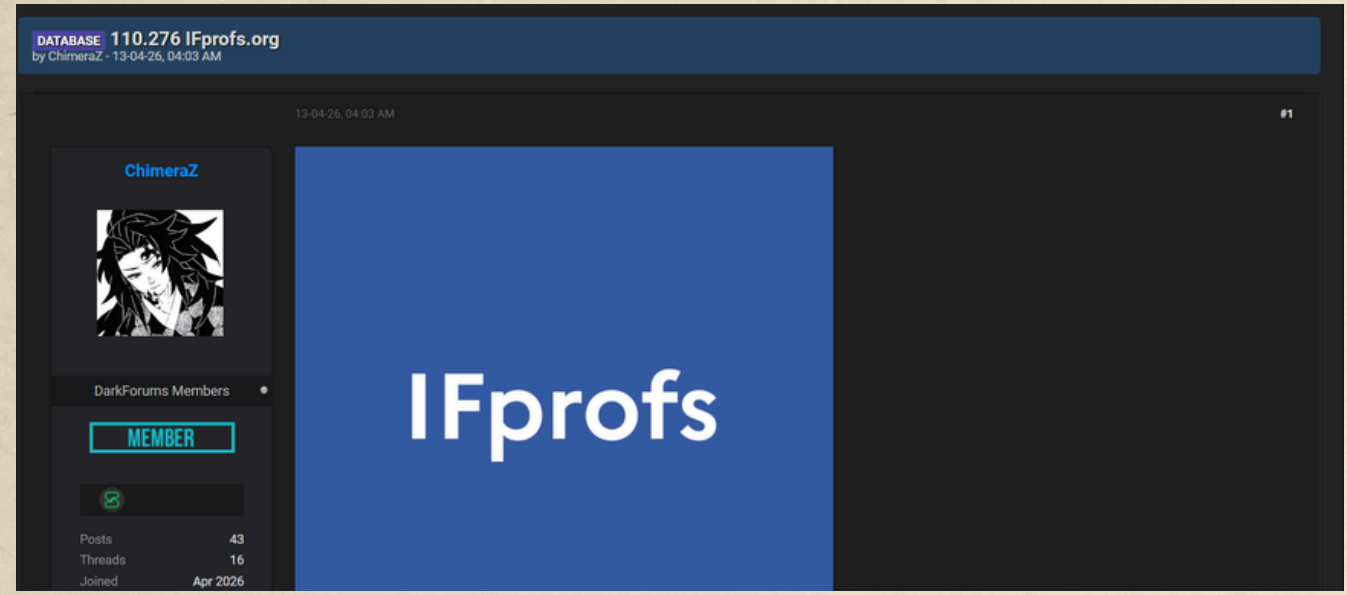
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 12 APR - 18 APR 2026

IDprofs Breach Incident

On April 13, 2026, IFprofs, a France-based organization in the Government / Education sector has experienced a notable data exposure affecting sensitive educational and administrative records.

Company Sector: Government
Threat Actor ChimeraZ
Data Sold: 42.8 Mb



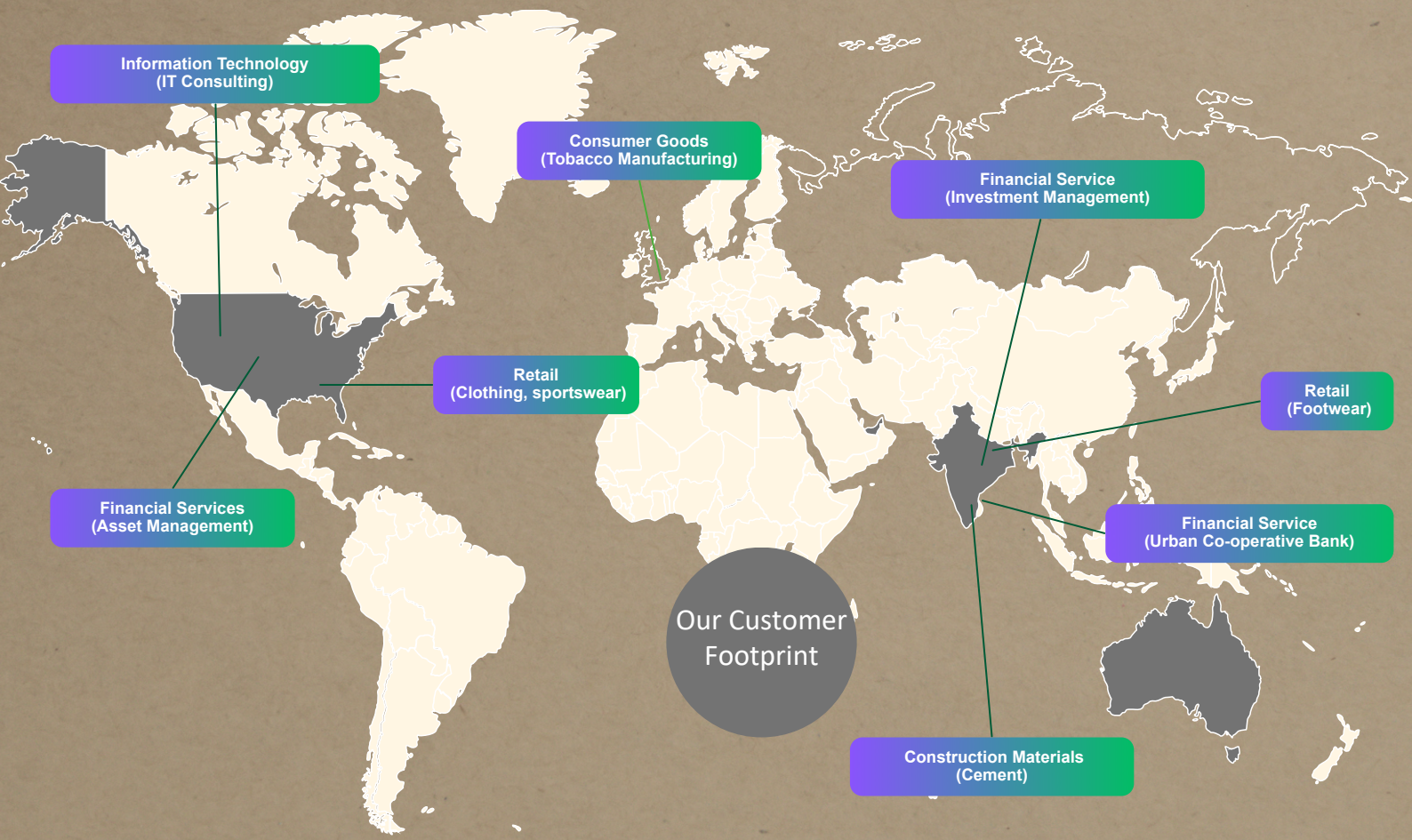
Key Highlights

- **Data Exposure:** Database records leaked, containing sensitive educational and administrative information
- **Source & Risk:** Shared on hidden underground forum; possible monetization
- **Threat Actor:** Linked to ChimeraZ
- **Threat Level:** Non-ransomware breach with risks of unauthorized access, data misuse, and impact on institutional systems and users

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