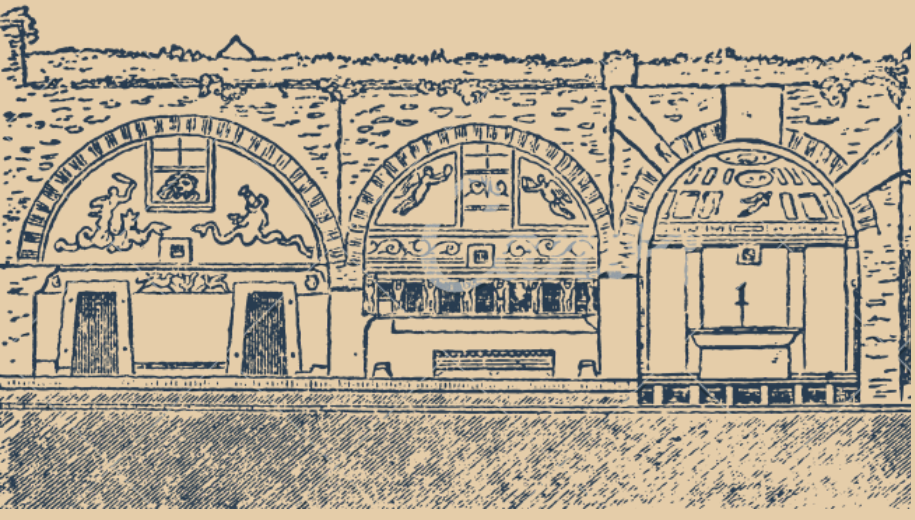
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 14 JUNE – 20 JUNE 2026



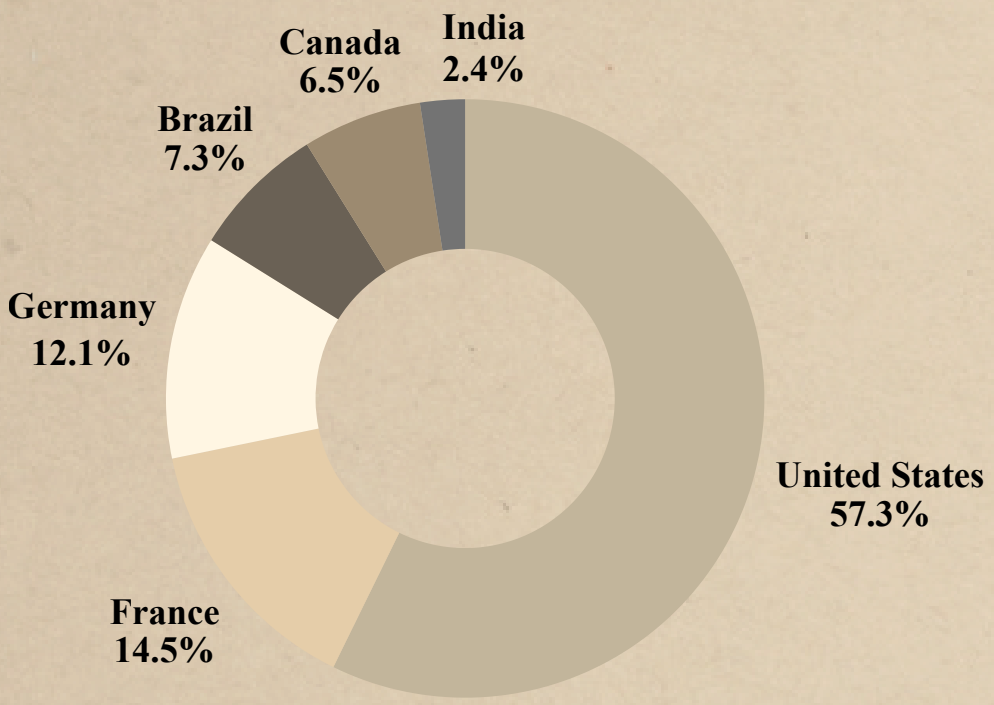
GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 14 JUNE - 20 JUNE 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 **LockBit, The Gentlemen**, **ShinyHunters**, and **Qilin** were most frequently observed, indicating sustained and coordinated attack campaigns.

Most Targeted Sector: Manufacturing

Total Breaches Observed: 244

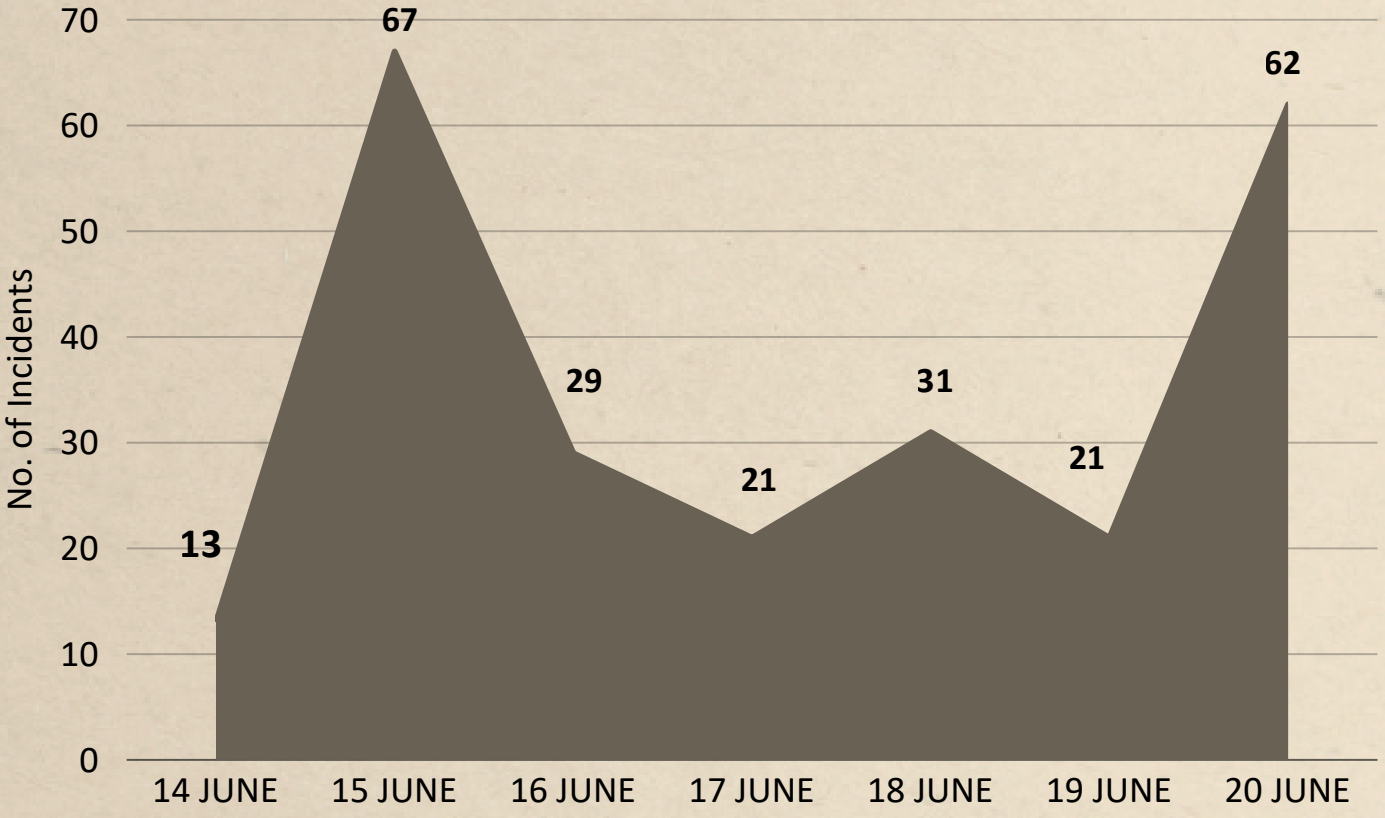
Ransomware-linked breaches: 82.8%

Countries Affected: 64

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD: 14 JUNE - 20 JUNE 2026

Breach Over time

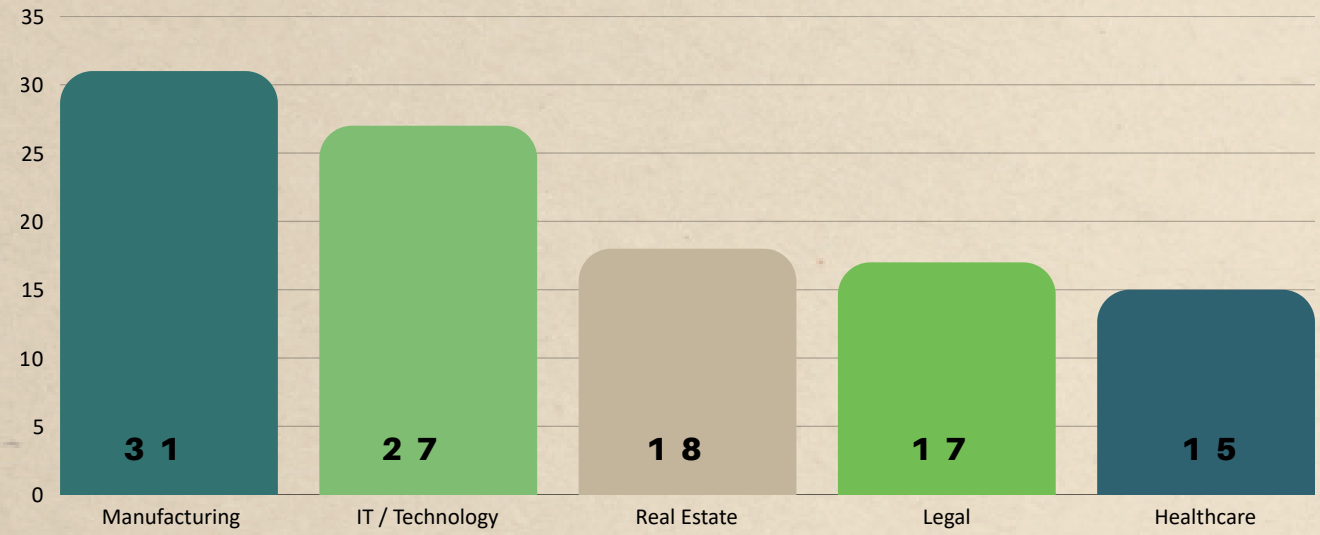


- Breach activity fluctuated throughout the period, with June 15, recording the highest spike at 67 reported incidents.
- A sharp rise was observed between June 18 and June 20, peaking at 62 incidents on June 20, indicating intensified disclosure or attack activity.
- June 14 reported the lowest number 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: 14 JUNE - 20 JUNE 2026

Affected Sectors



Industry Highlights

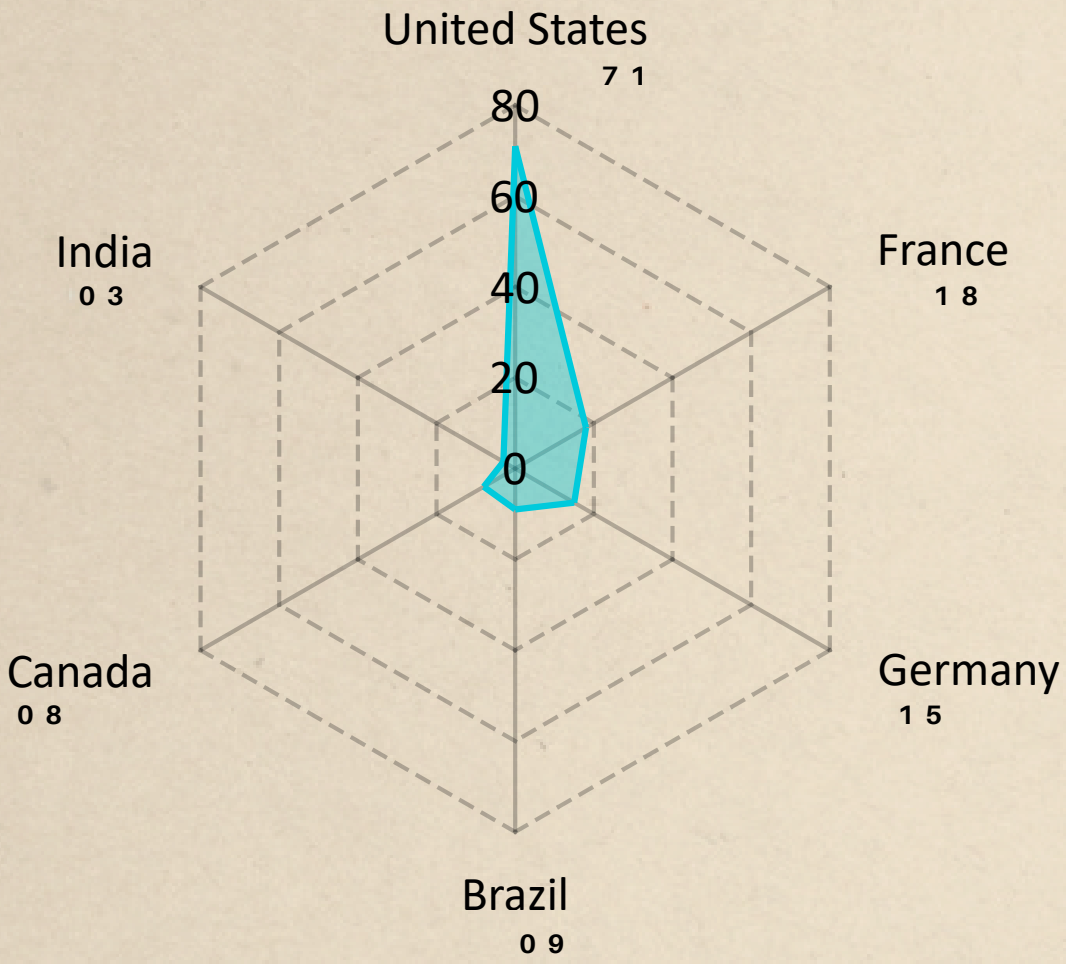
- **Manufacturing & Engineering: 31+ incidents (highest targeted sector)**
- **IT / Technology: 27+ incidents (high exposure due to digital infrastructure)**
- **Real Estate : 18+ incidents**
- **Legal : 17+ incidents**
- **Healthcare : 15+ incidents**

Industries Insight: Manufacturing and technology sectors remained the most frequently targeted, while construction, finance, and healthcare continued to experience elevated activity due to their critical operations, extensive digital ecosystems, and valuable data holdings.

GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 14 JUNE - 20 JUNE 2026

Affected Countries



Actor Distribution

Ransomware dominates the threat landscape with 202+ incidents, far outpacing 42 non-ransomware cases, making it the most prevalent and impactful attack type.

GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:14JUNE-20JUNE 2026

Tata Electronics Breach Incident

On June 10, 2026, a **Indian company Tata Electronics** suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Technology
Threat Group (Ransomware) : Worldleaks
Data Sold: 600+ GB

Key Highlights

- **Data Exposure:** Tata Electronics was listed by the WorldLeaks ransomware group, with claims of unauthorized access to company systems and data.
- **Threat Actor:** Linked to **WorldLeaks**
- **Threat Activity:** WorldLeaks added the company to its leak site and announced the incident as part of its extortion operation.
- **Threat Level:** High – Potential exposure of sensitive corporate information could lead to operational disruption, reputational damage, targeted phishing, and supply-chain risks.

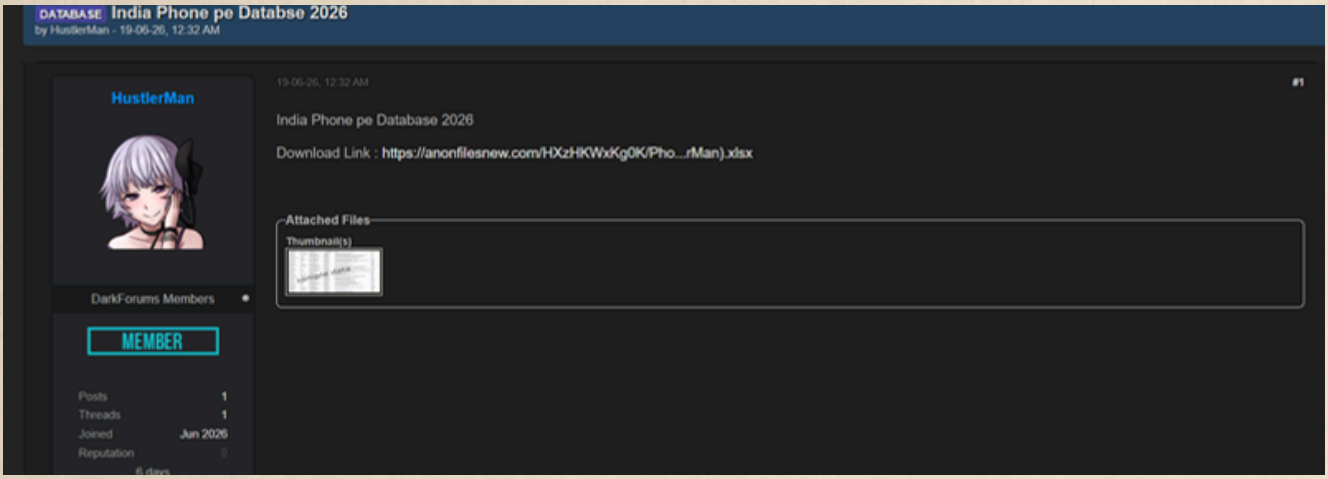
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:14JUNE-20JUNE 2026

PhonePe Limited Breach Incident

On June 19, 2026, a **Indian company PhonePe Limited** suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Fintech / Digital Payments
Threat Actor : HustlerMan
Data Sold: 946 KB



Key Highlights

- **Data Exposure: :** Alleged PhonePe India database shared on a cybercrime forum, with downloadable XLSX file references.
- **Threat Actor:** Posted by **HustlerMan**
- **Threat Activity :** Data leak / database distribution targeting PhonePe-related user information.
- **Threat Level:** Medium to High, depending on the authenticity and sensitivity of the exposed records.

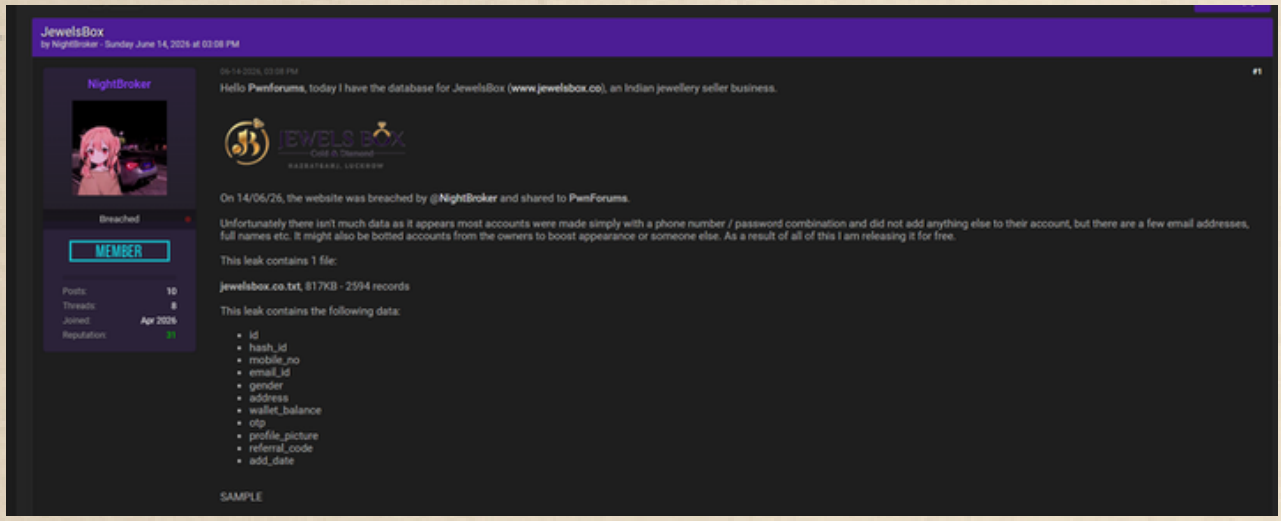
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:14JUNE-20JUNE 2026

Jewels Box Breach Incident

On June 14, 2026, a **Indian company Jewels Box** suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: **Retail (Gold, Diamond, and Silver Jewelry)**
Threat Actor : **NightBroker**
Data Sold: **817KB**



Key Highlights

- **Data Exposure:** Alleged JewelsBox customer database containing 2,594 records was shared on a cybercrime forum.
- **Threat Actor:** Linked to **NightBroker**
- **Threat Activity:** Data breach and public distribution of an alleged customer database.
- **Threat Level:** Medium to High due to risks of phishing, account misuse, identity theft, and targeted scams.

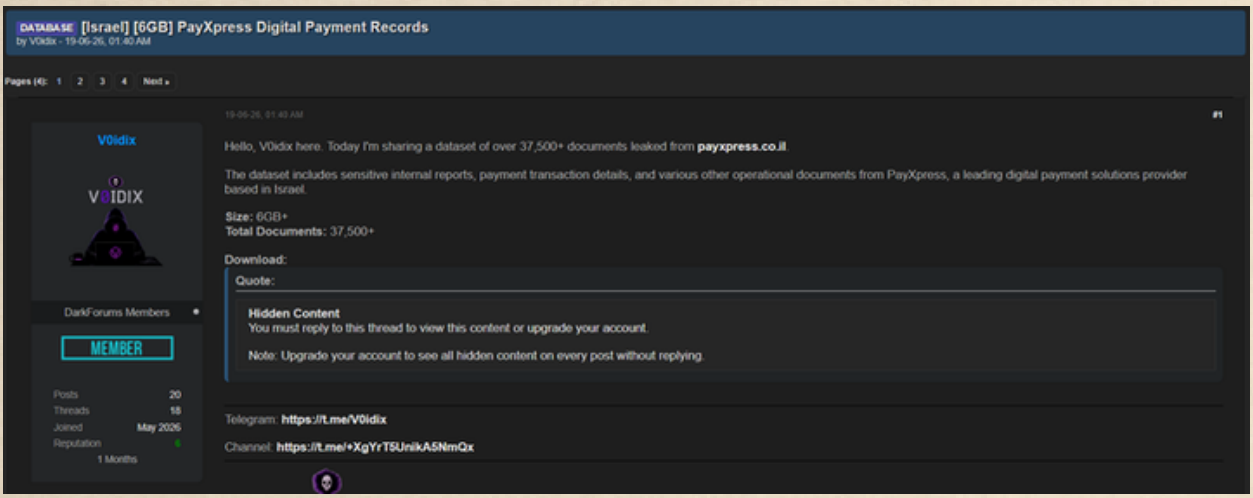
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD: 14 JUNE - 20 JUNE 2026

PayXpress Breach Incident

On June 19, 2026, a **Israel company PayXpress** suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Fintech / Pre-paid Payment Technology
Threat Actor : V0idix
Data Sold: 6GB+



Key Highlights

- **Data Exposure:** Alleged 6GB+ PayXpress dataset containing over 37,500 internal documents was advertised on a cybercrime forum.
- **Threat Activity:** Data leak and public distribution of alleged internal corporate and payment-related records.
- **Threat Actor:** Linked to **V0idix**
- **Threat Level:** High due to potential financial fraud, business intelligence exposure, phishing, and operational security risks.

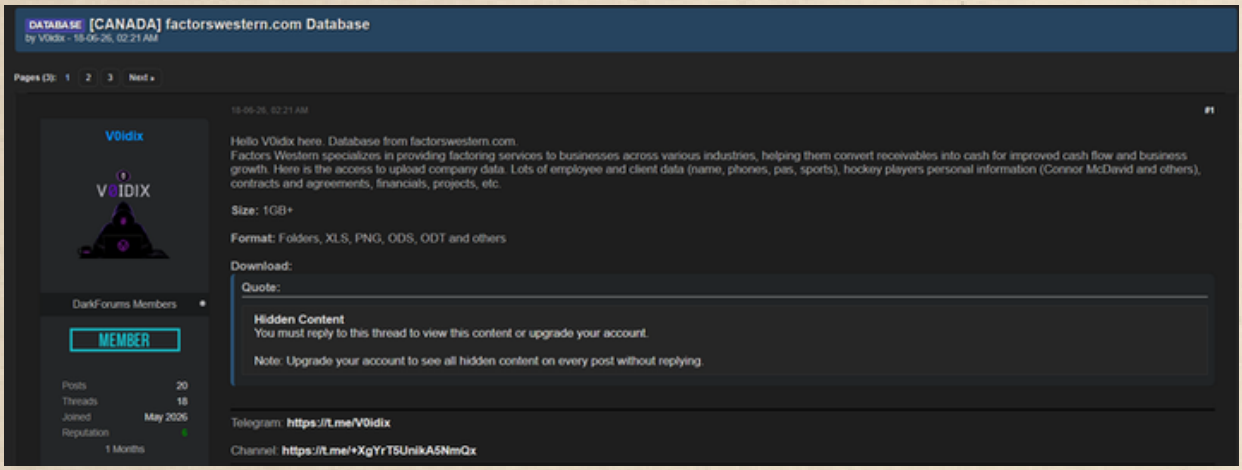
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:14JUNE-20JUNE 2026

Factors Western Inc. Breach Incident

On June 18, 2026, a **Canada company Factors Western Inc.** suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Financial Services
Threat Actor : V0idix
Data Sold: 1GB+



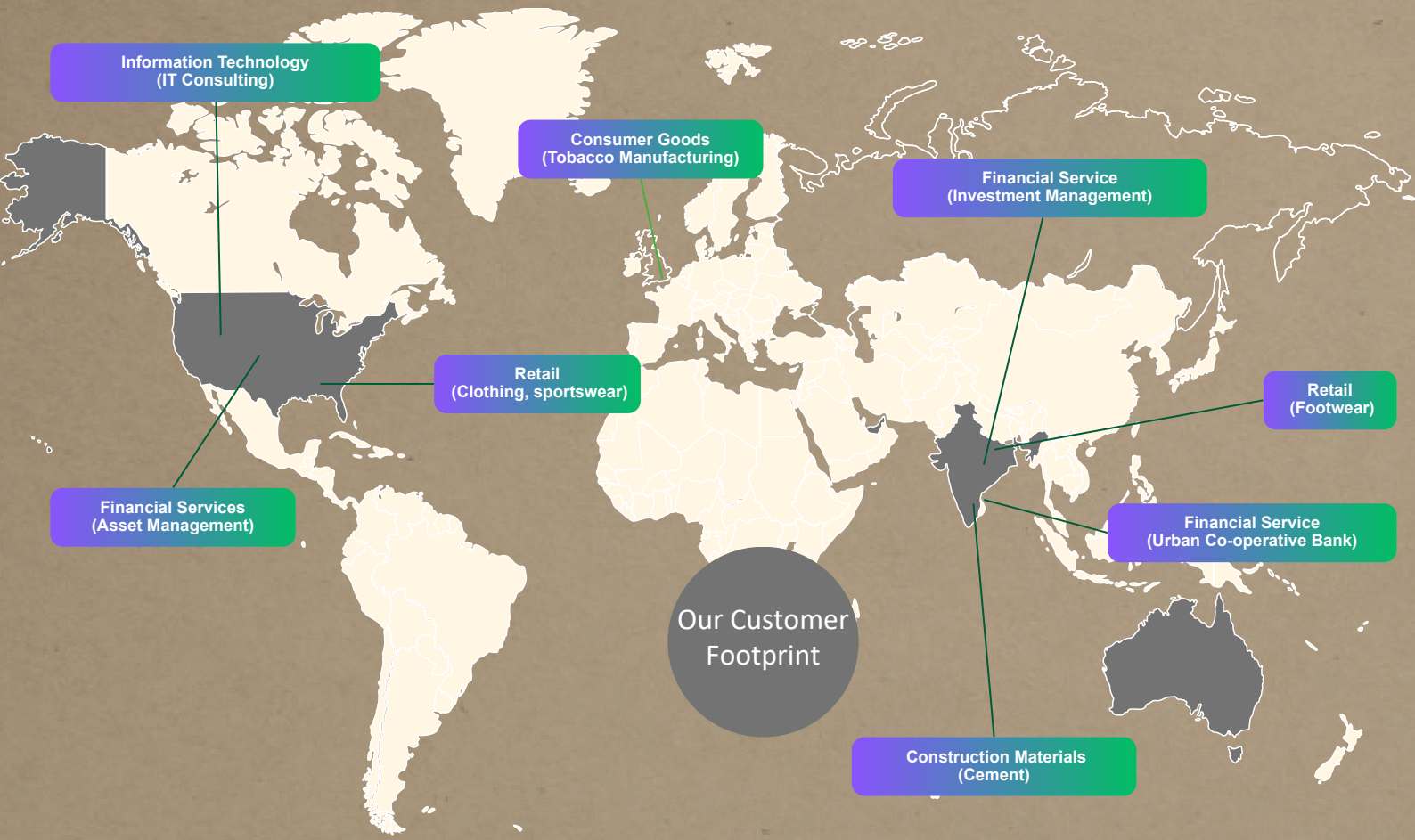
Key Highlights

- **Data Exposure:** Alleged 1GB+ Factors Western database was advertised on a cybercrime forum, containing employee, client, financial, and business-related records.
- **Threat Actor:** Linked to **V0idix**
- **Threat Activity:** Data leak and public distribution of alleged corporate and customer information.
- **Threat Level:** High due to risks of identity theft, financial fraud, corporate espionage, phishing, and unauthorized access to sensitive business data.

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