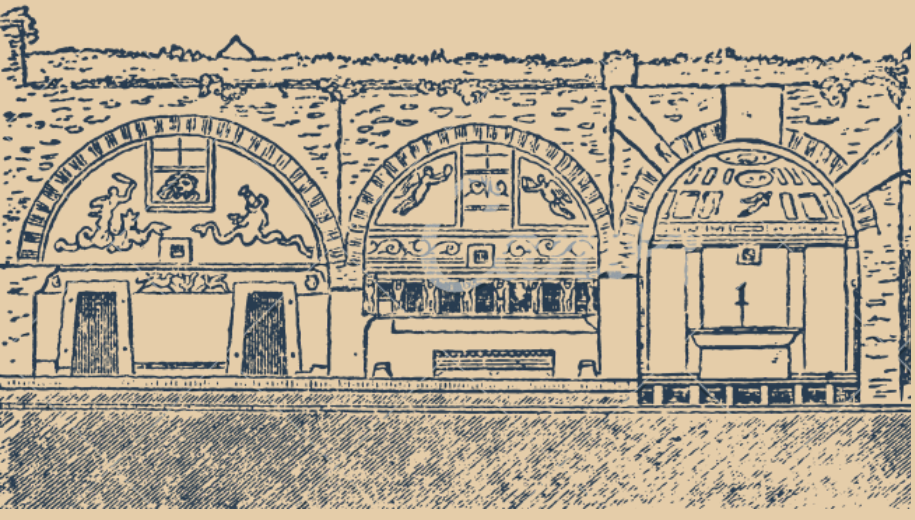
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 21 JUNE – 27 JUNE 2026



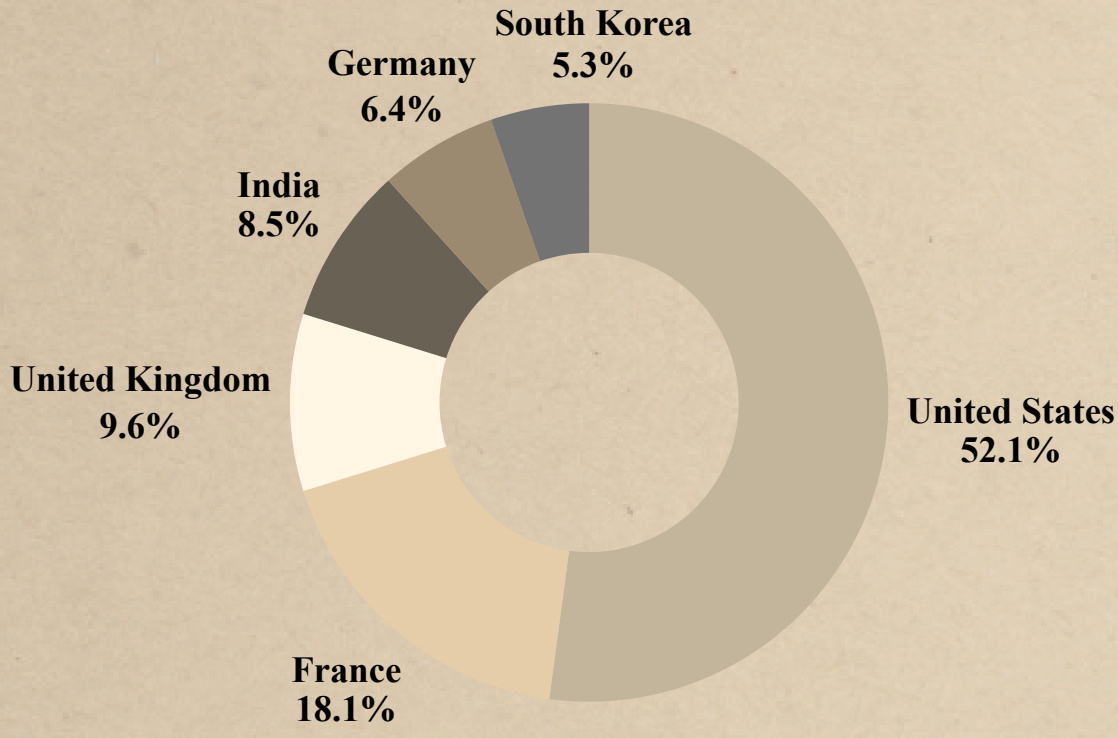
GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 21 JUNE - 27 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, reflecting the continued dominance of financially motivated cyber threats.
- Threat groups such as **Nova, Qilin, Stormous**, and **InCransom** were most frequently observed, indicating sustained and coordinated attack campaigns.

Most Targeted Sector: Manufacturing

Ransomware-linked breaches: 58.1%

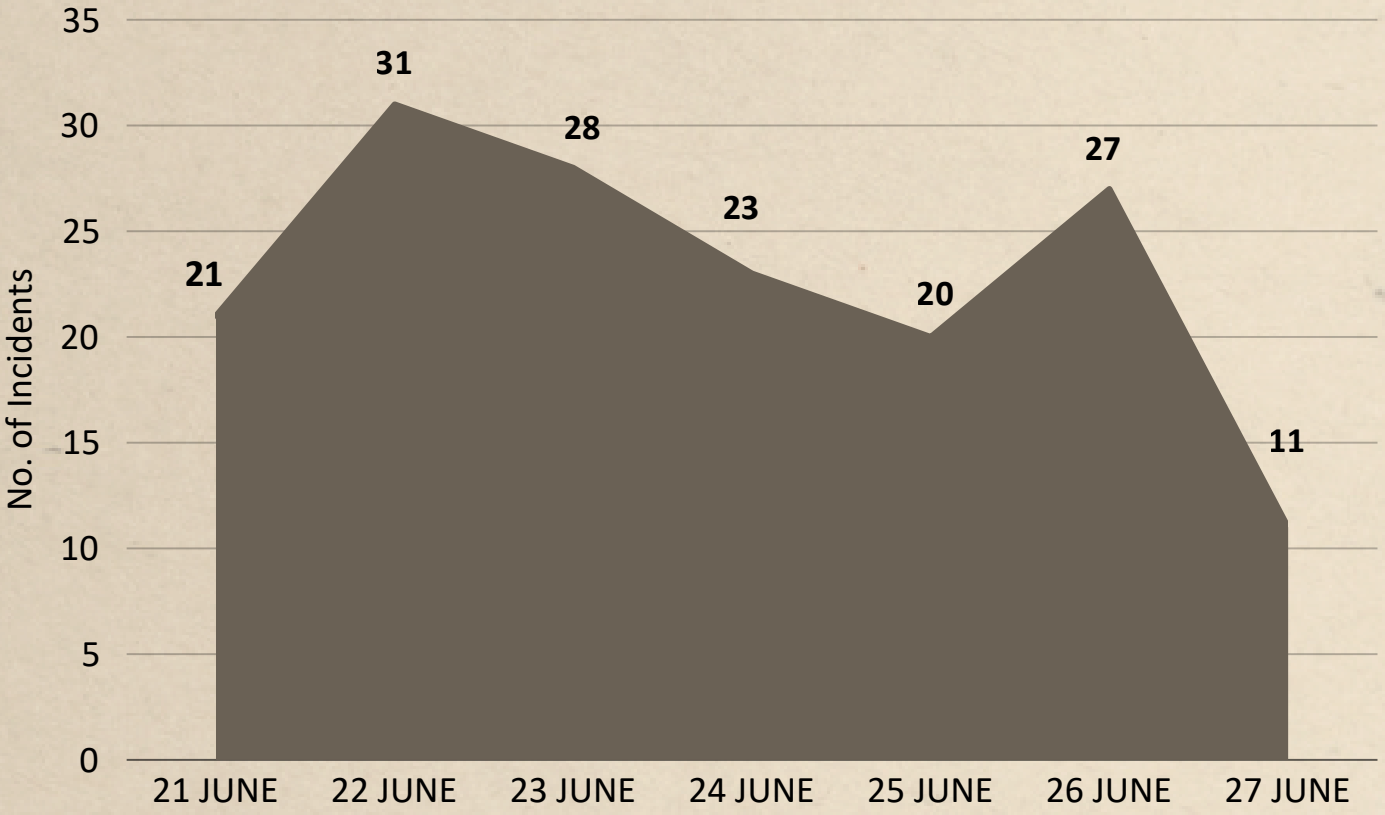
Total Breaches Observed: 160

Countries Affected: 49

GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD: 21 JUNE - 27 JUNE 2026

Breach Over time

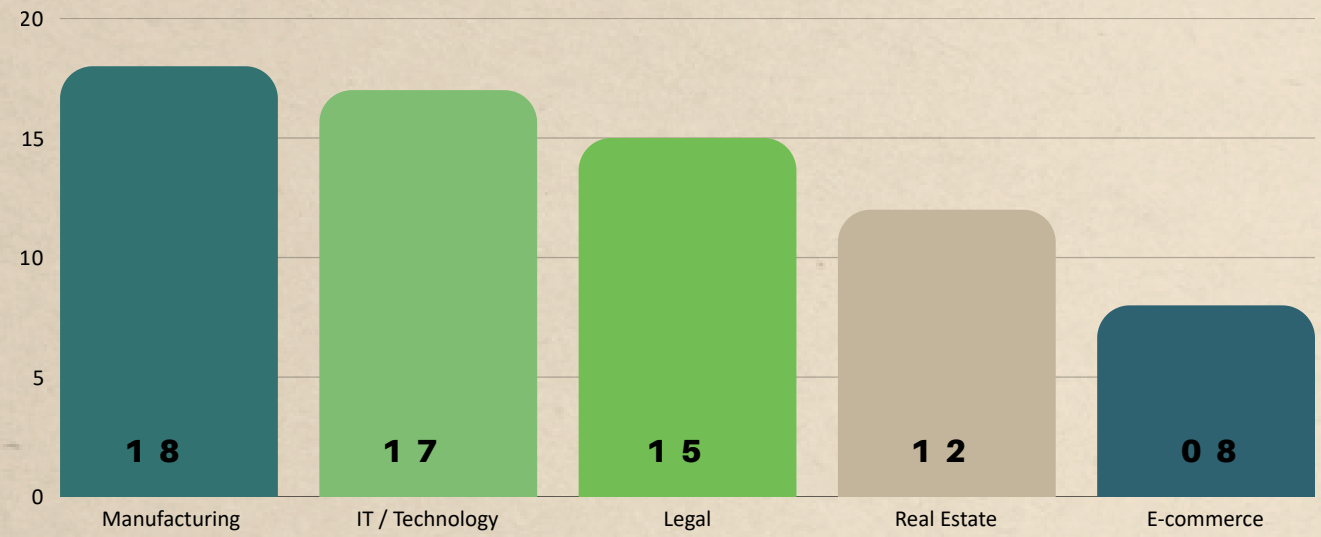


- Breach activity fluctuated throughout the period, with June 22, recording the highest spike at 31 reported incidents.
- A sharp rise was observed between June 23 and June 26, peaking at 28 incidents on June 23, indicating intensified disclosure or attack activity.
- June 27 reported the lowest number of incidents, with only 11 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: 21 JUNE - 27 JUNE 2026

Affected Sectors



Industry Highlights

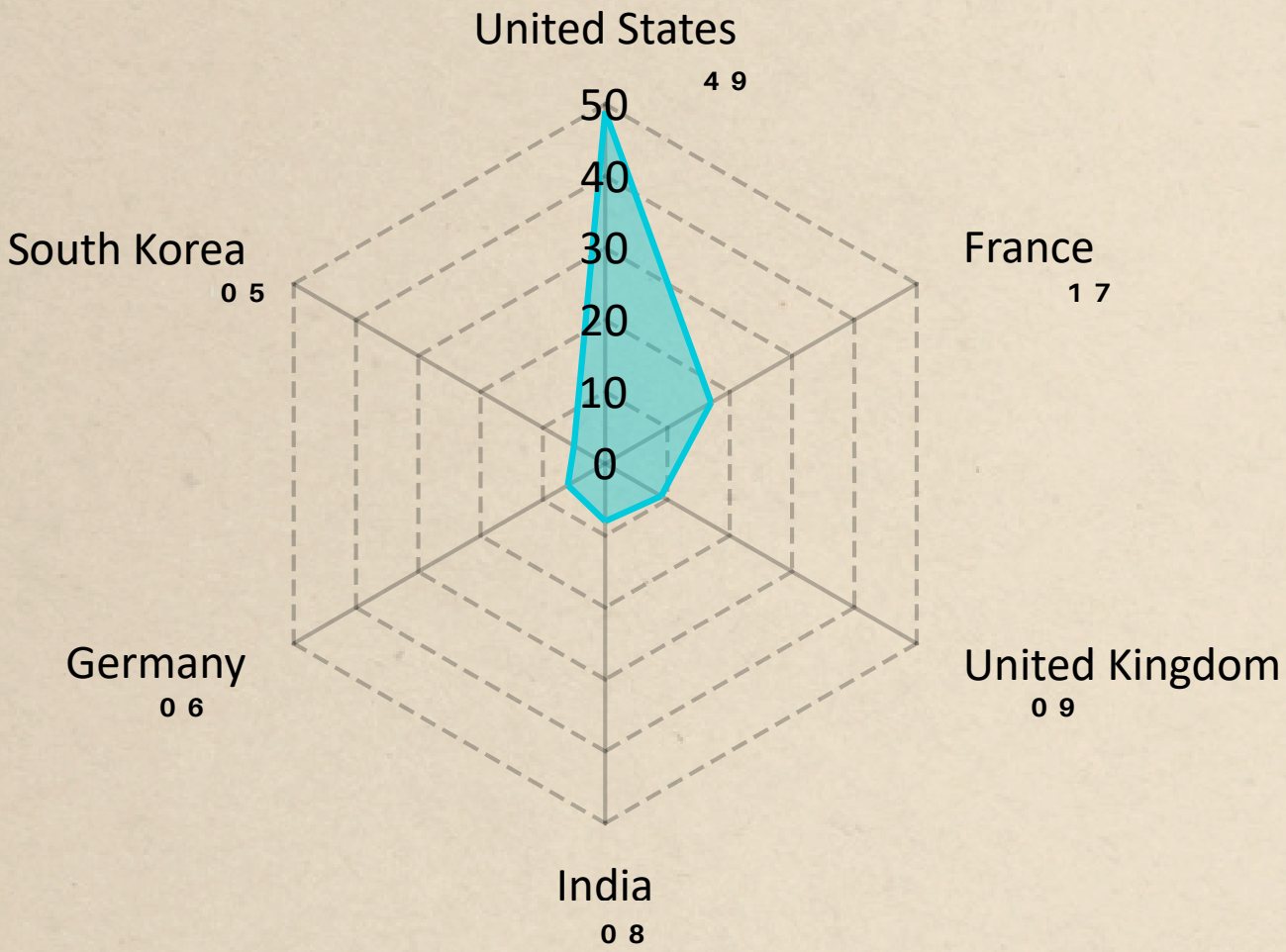
- **Manufacturing & Engineering: 18+ incidents (highest targeted sector)**
- **IT / Technology: 17+ incidents (high exposure due to digital infrastructure)**
- **Legal : 15+ incidents**
- **Real Estate : 12+ incidents**
- **E-Commerce : 08+ incidents**

Industries Insight: Manufacturing remained the most frequently targeted sector, closely followed by technology and financial services. Construction and retail organizations also experienced sustained activity, highlighting attackers' continued focus on industries with critical operations, digital infrastructure, and valuable business data.

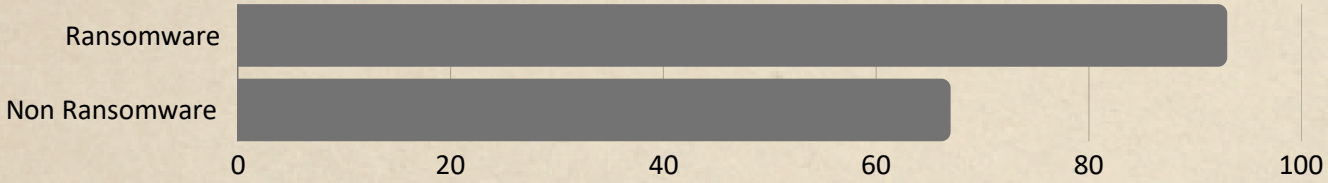
GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 21 JUNE - 27 JUNE 2026

Affected Countries



Actor Distribution



Ransomware dominates the threat landscape with 93+ incidents, far outpacing 67 non-ransomware cases, making it the most prevalent and impactful attack type.

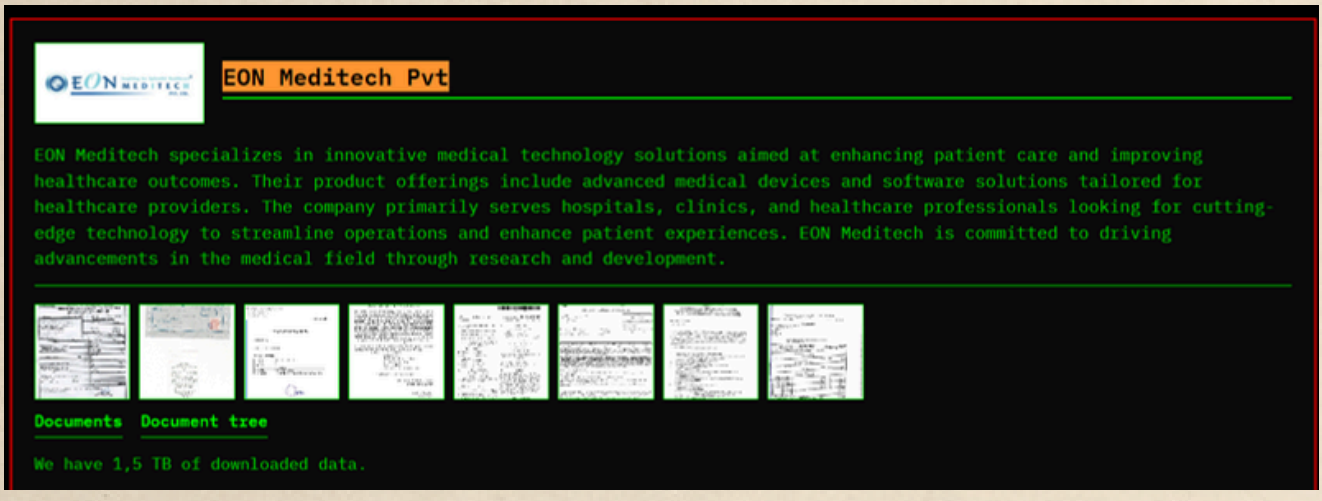
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:21JUNE-27JUNE 2026

EON Meditech Pvt Breach Incident

On June 22, 2026, a **Indian company EON Meditech Pvt** suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Healthcare / Medicine
Threat Group (Ransomware) : cmdorganization
Data Sold: 1.5 TB



Key Highlights

- **Data Exposure:** Alleged 1.5 TB of EON Meditech data was claimed to have been exfiltrated and published on a ransomware leak site.
- **Threat Group:** Linked to **cmdorganization**
- **Source & Risk:** The leak reportedly includes corporate documents, certificates, and business records with document previews provided.
- **Threat Activity:** Public disclosure of alleged stolen corporate data as part of a data extortion campaign.
- **Threat Level:** High due to potential exposure of sensitive business information, regulatory risks, and possible misuse of confidential documents.

GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD:21JUNE-27JUNE 2026

VSL Marine Technology Breach Incident

On June 26, 2026, a **Indian company VSL Marine Technology** suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: **3D scanning and engineering services**
Threat Group (Ransomware) : **Nova**
Data Sold: **510 GB**

Key Highlights

- **Data Exposure:** Alleged 510 GB of VSL Marine Technology Pvt. Ltd. data was listed on a ransomware leak site.
- **Threat Group :** Posted by **Nova**
- **Source & Risk:** The leak reportedly includes engineering-related files and company data profiles available for download.
- **Threat Activity :** Public disclosure and distribution of alleged stolen corporate data as part of a data extortion campaign.
- **Threat Level:** High due to potential exposure of proprietary engineering data, business information, and operational documents.

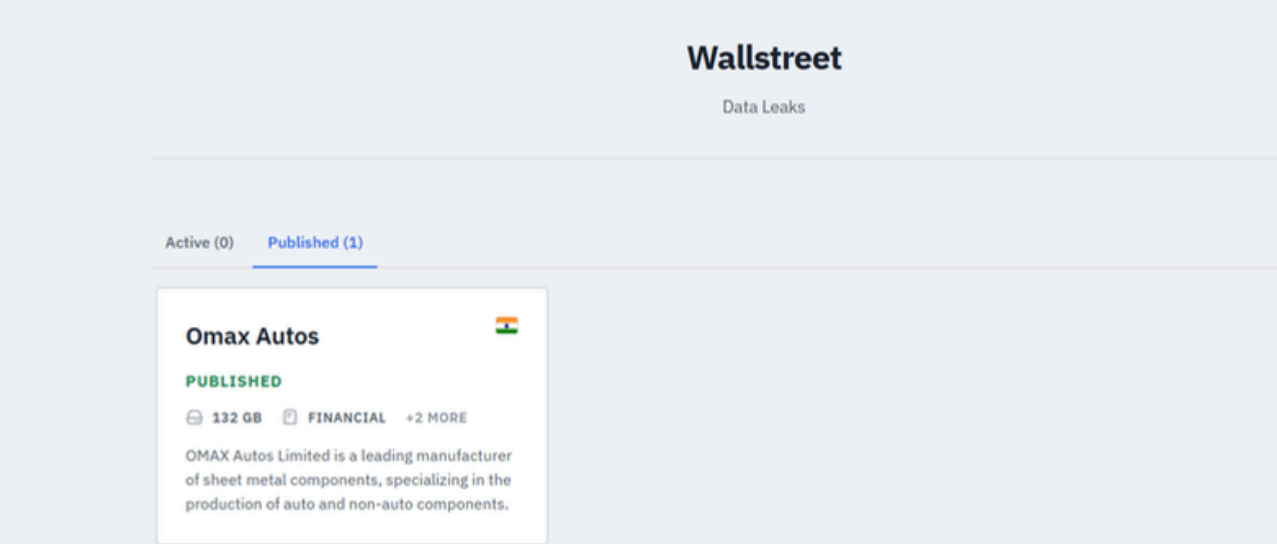
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD:21JUNE-27JUNE 2026

Omax Autos Ltd. Breach Incident

On June 26, 2026, a **Indian company Omax Autos Ltd.** suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Automotive
Threat Group (Ransomware) : Wallstreet
Data Sold: 132 GB



Key Highlights

- **Data Exposure:** Alleged 132 GB of Omax Autos data was published on a ransomware leak site.
- **Threat Actor:** Linked to **Wallstreet**
- **Source & Risk:** The leak reportedly contains financial records and additional corporate data available for download.
- **Threat Activity:** Public disclosure of alleged stolen corporate data as part of a data extortion campaign
- **Threat Level:** High due to potential exposure of financial information, confidential business records, and operational data.

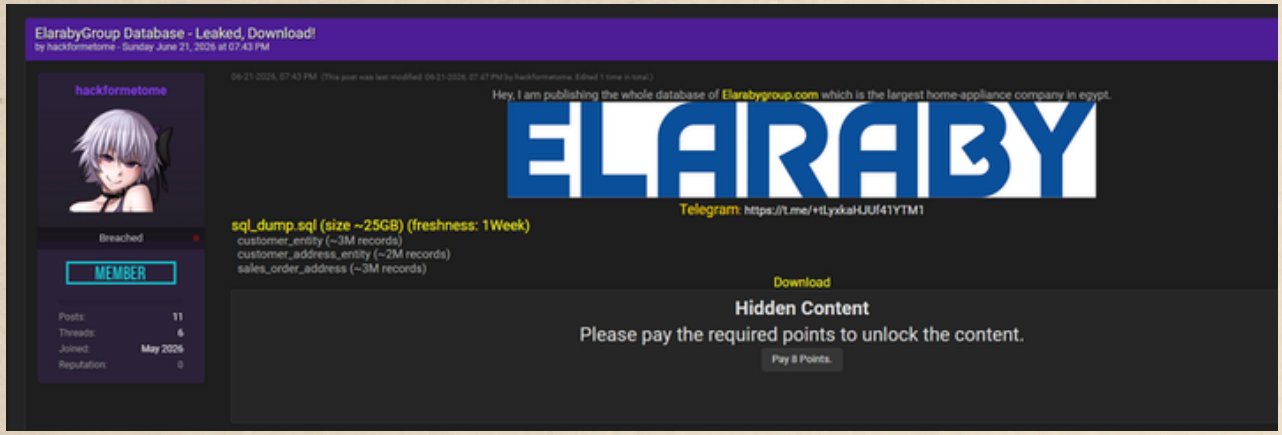
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:21JUNE-27JUNE 2026

El-Araby Group Breach Incident

On June 21, 2026, an **Egypt Company El-Araby Group** suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Consumer Electronics and Home Appliances
Threat Actor : hackformetome
Data Sold: 25 GB



Key Highlights

- **Data Exposure:** Alleged ~25 GB SQL database of Elaraby Group was published on a cybercrime forum.
- **Threat Activity:** Public disclosure and attempted distribution of alleged stolen corporate data via a cybercrime forum as part of a data extortion campaign.
- **Threat Actor:** Linked to **hackformetome**
- **Source & Risk:** The dataset reportedly contains customer, address, and sales order databases comprising millions of records.
- **Threat Level:** High due to the potential exposure of customer data, business records, and operational information.

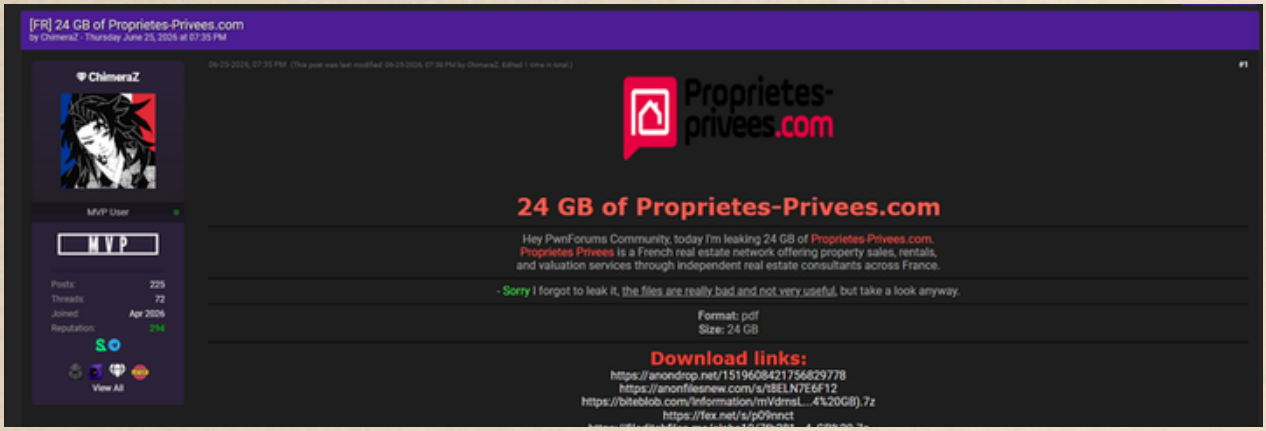
GLOBAL DATA BREACH REPORT

✱ REPORTING PERIOD:21JUNE-27JUNE 2026

Proprietes-Privees.com Breach Incident

On June 25, 2026, a **France company Proprietes-Privees.com** suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Real Estate (Real Estate Agency Network)
Threat Actor : ChimeraZ
Data Sold: 24 GB



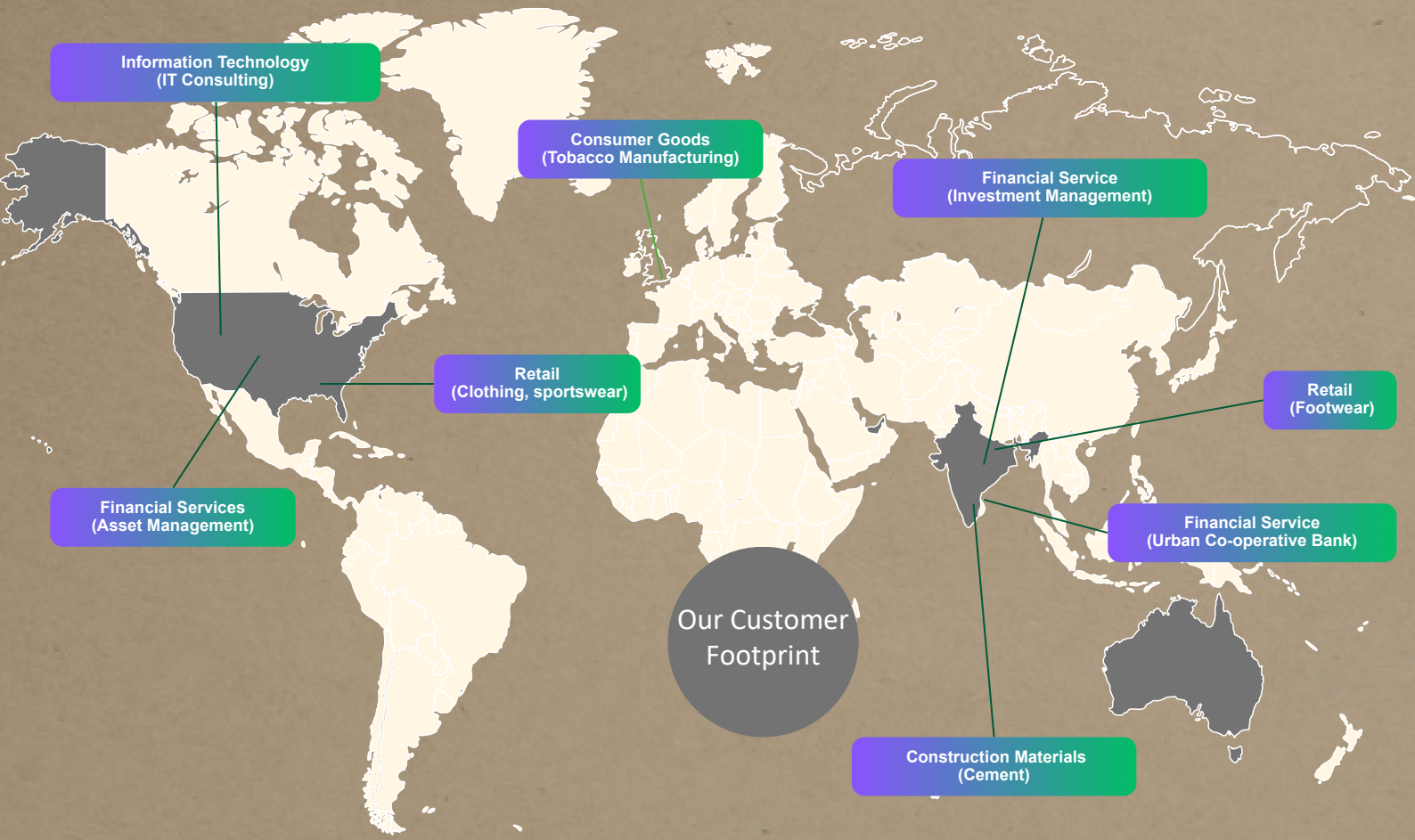
Key Highlights

- **Data Exposure:** Alleged 24 GB dataset of Proprietes-Privees.com was published on a cybercrime forum.
- **Threat Actor:** Linked to **ChimeraZ**
- **Source & Risk:** The leaked archive, reportedly in PDF format, was made available through multiple download links.
- **Threat Activity:** Public disclosure and distribution of alleged stolen corporate data as part of a data leak campaign.
- **Threat Level:** High due to the potential exposure of sensitive business documents and proprietary 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