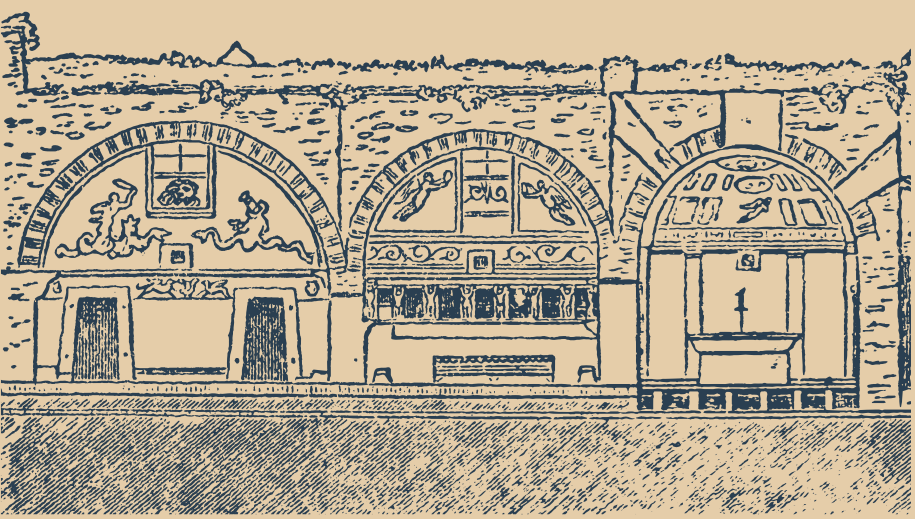
CASTELLUM LABS

WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 19 APR – 02 MAY 2026



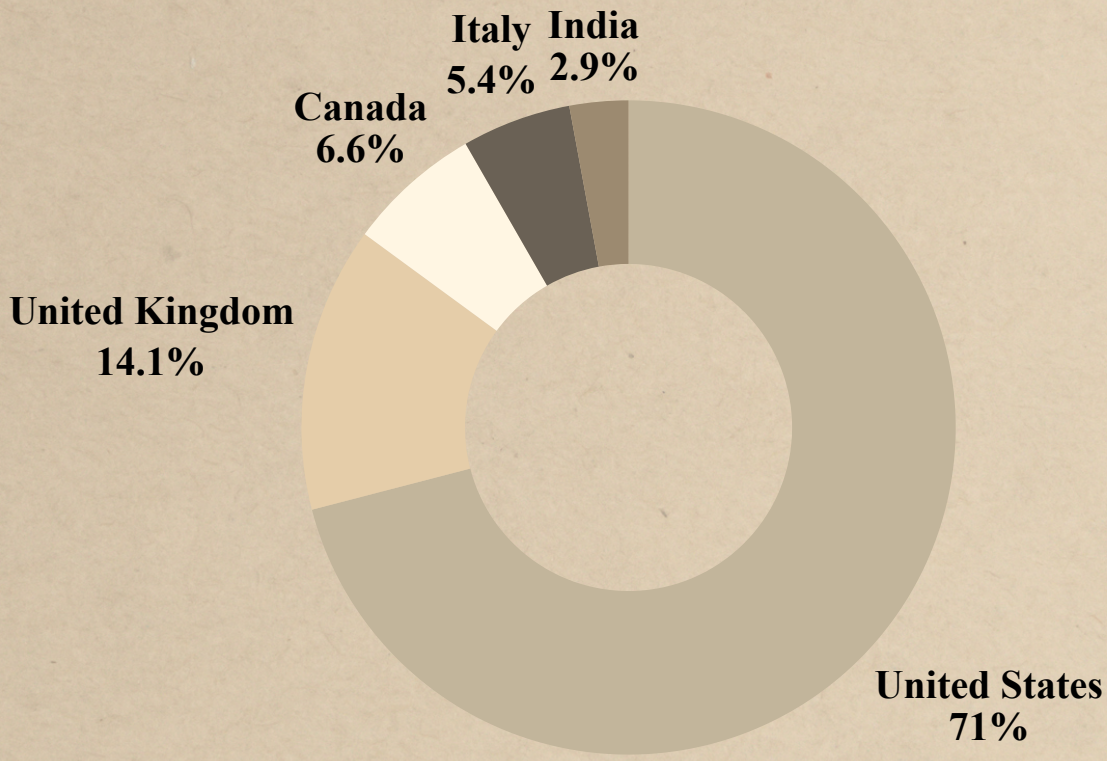
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 19 APR - 02 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 rise of financially motivated cyberattacks.
- Threat groups such as Qilin, APT73, DragonForce, and Incransom were repeatedly observed, indicating sustained and coordinated malicious campaigns.

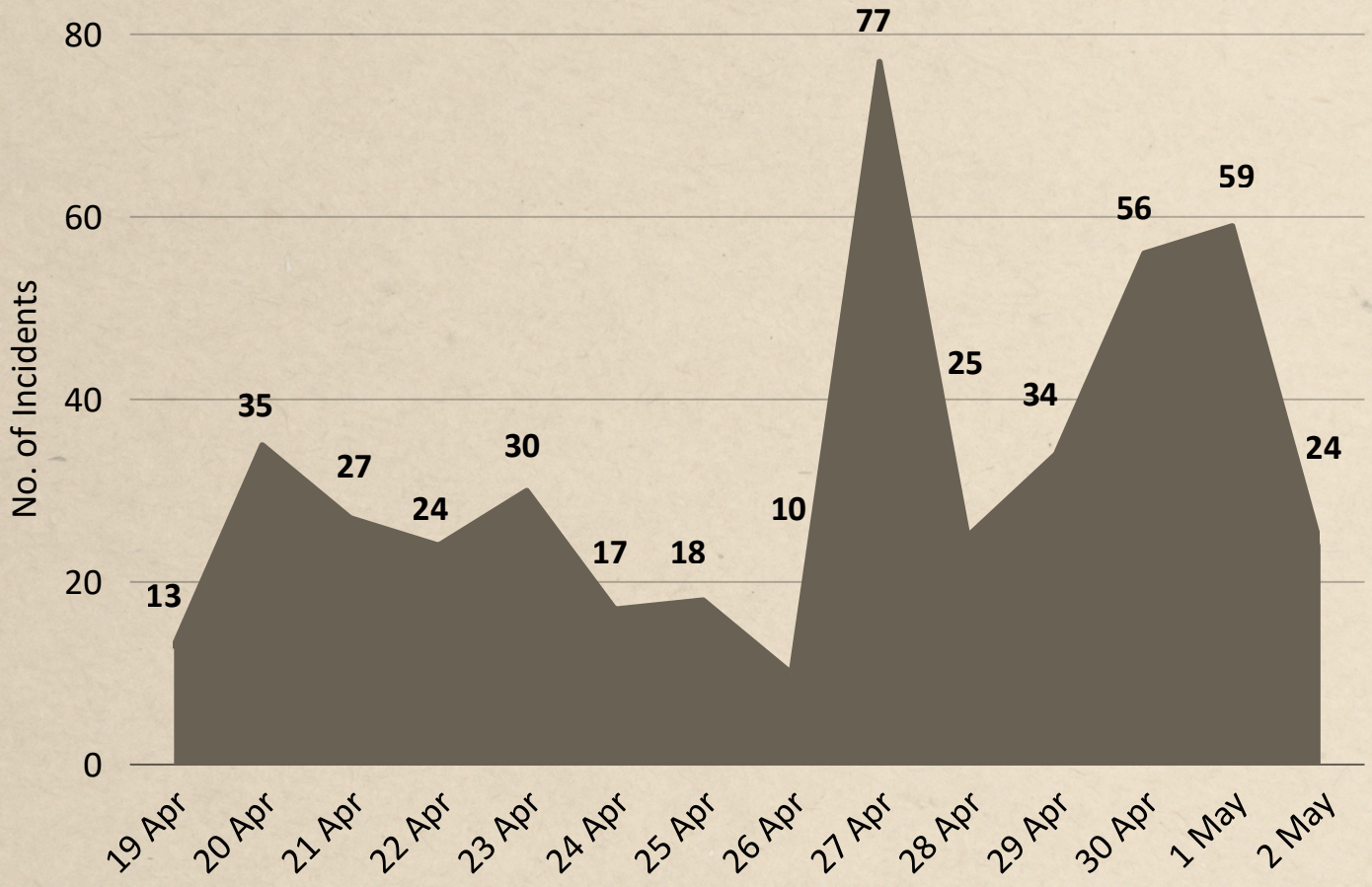
Most Targeted Sector: Manufacturing
Ransomware-linked breaches: 93.1%

Total Breaches Observed: 449
Countries Affected: 67

GLOBAL DATA BREACH REPORT

REPORTING PERIOD: 19 APR - 02 MAY 2026

Breach Over time

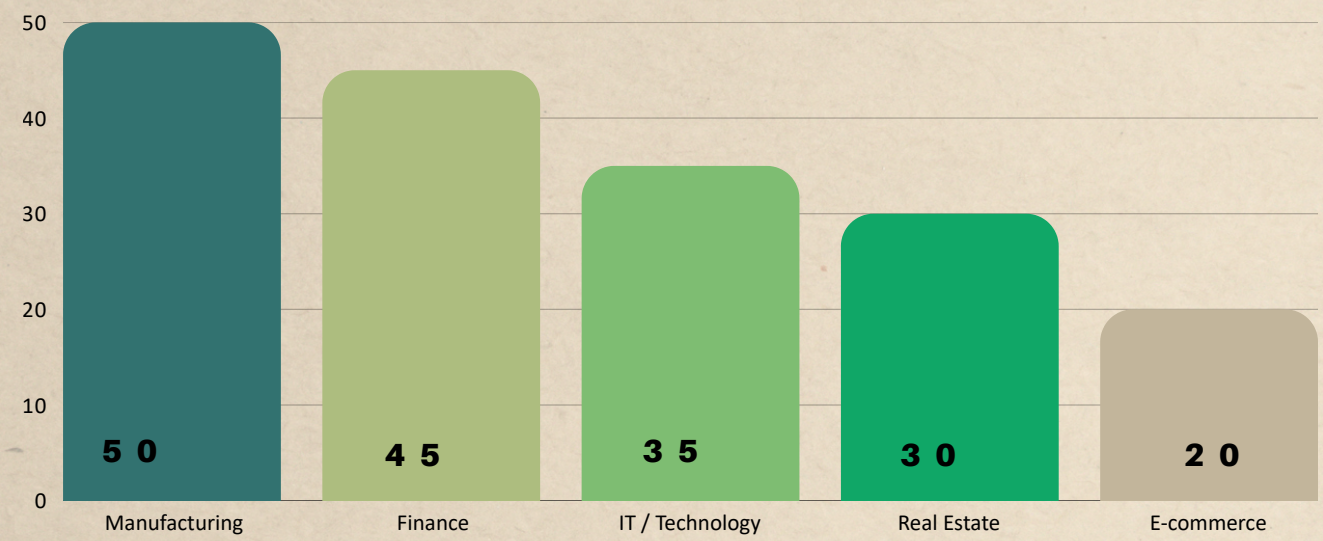


- Breach activity fluctuated throughout the period, with April 27 recording the highest spike at 77 reported incidents.
- A sharp rise was observed between April 29 and May 1, peaking at 59 incidents on May 1, indicating intensified disclosure or attack activity.
- April 26 reported the lowest number of incidents, with only 10 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: 19 APR - 02MAY 2026

Affected Sectors



Industry Highlights

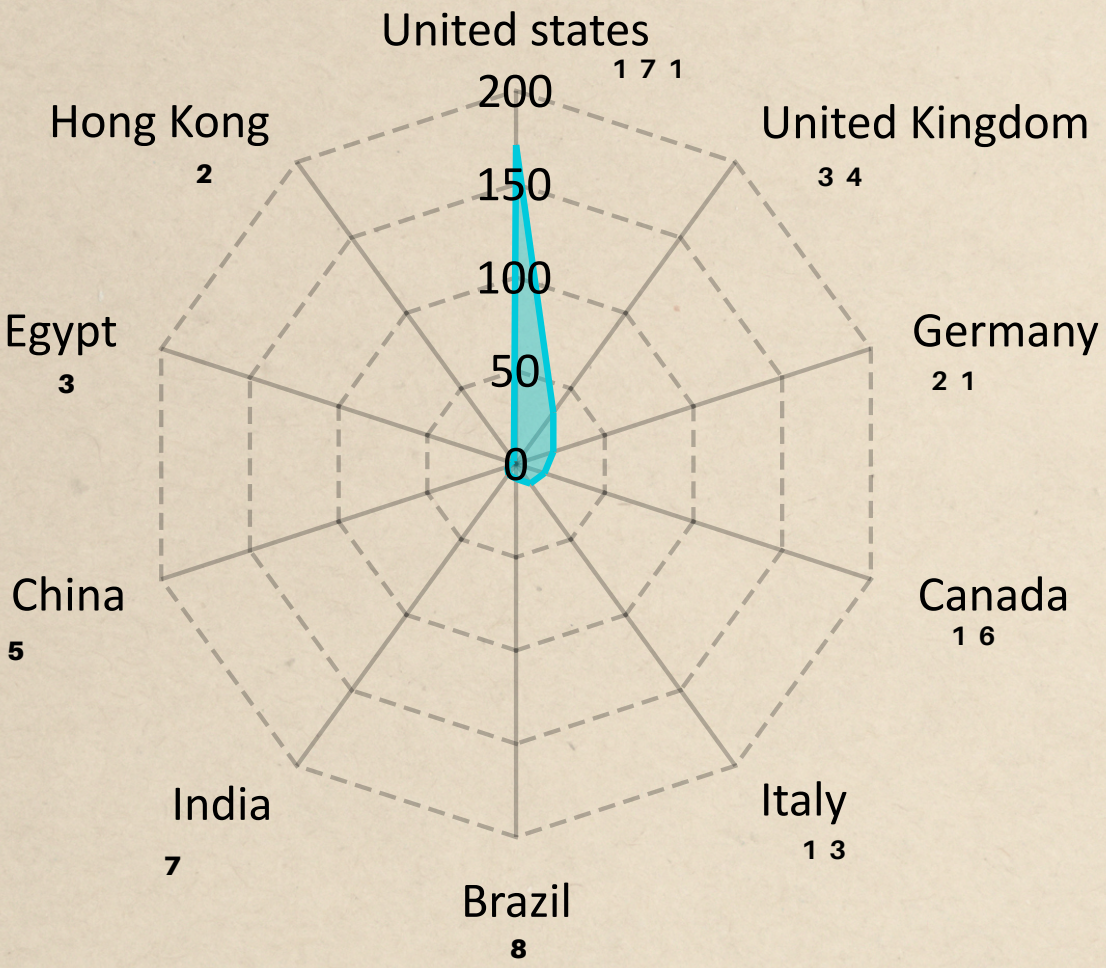
- **Manufacturing & Engineering: 50+ incidents (highest targeted sector)**
- **Finance / Legal / Insurance: 45+ incidents**
- **IT / Technology: 35+ incidents (high exposure due to digital infrastructure)**
- **Construction & Real Estate: 30+ incidents**
- **Retail & E-commerce: 20+ incidents**

Industries Insight: Manufacturing, financial, technology, and infrastructure-driven sectors remained the primary targets for ransomware and extortion-focused threat actors.

GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD: 19 APR - 02 MAY 2026

Affected Countries



Actor Distribution

Ransomware dominates the threat landscape with 418+ incidents, far outpacing 31 non-ransomware cases, making it the most prevalent and impactful attack type.

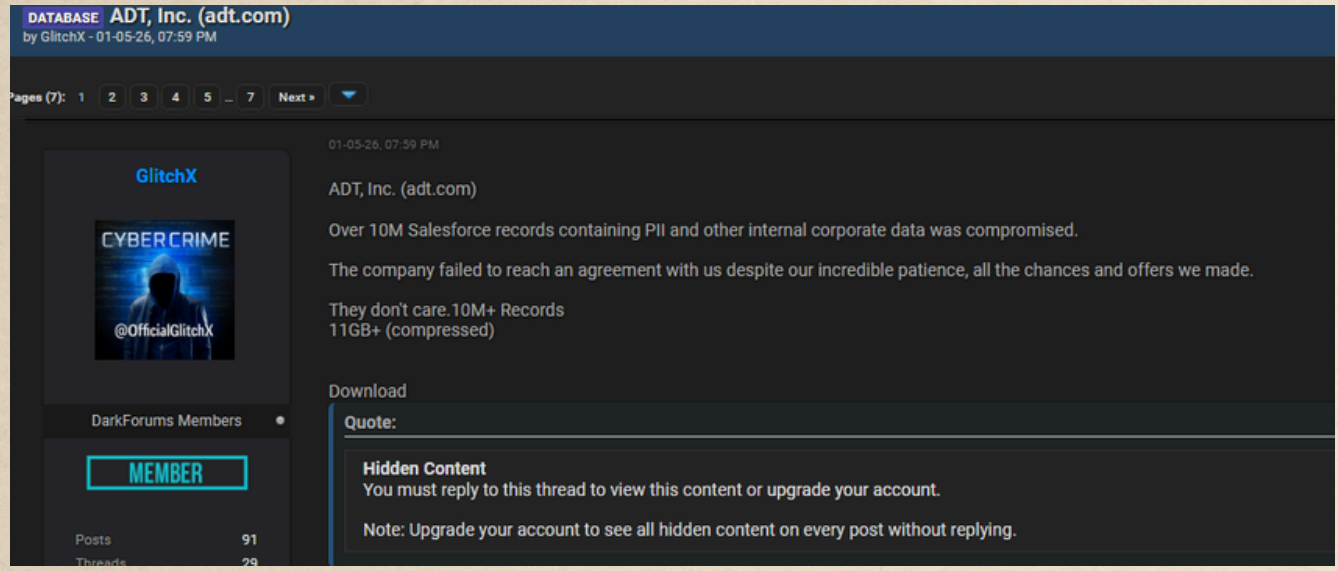
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD: 19 APR - 02 MAY 2026

ADT Inc Breach Incident

On May 01, 2026, a US company ADT Inc suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: **Safety and Security / Smart Home Technology**
Threat Actor : **GlitchX**
Data Sold: **11 GB**



Key Highlights

- **Data Exposure:** Over 10M Salesforce records reportedly compromised, including PII and internal corporate data
- **Threat Actor:** Claimed by GlitchX on underground cybercrime forum
- **Threat Activity:** Alleged failed negotiation attempts prior to data leak disclosure
- **Threat Level:** High-risk exposure with potential for identity misuse, unauthorized access, and reputational damage

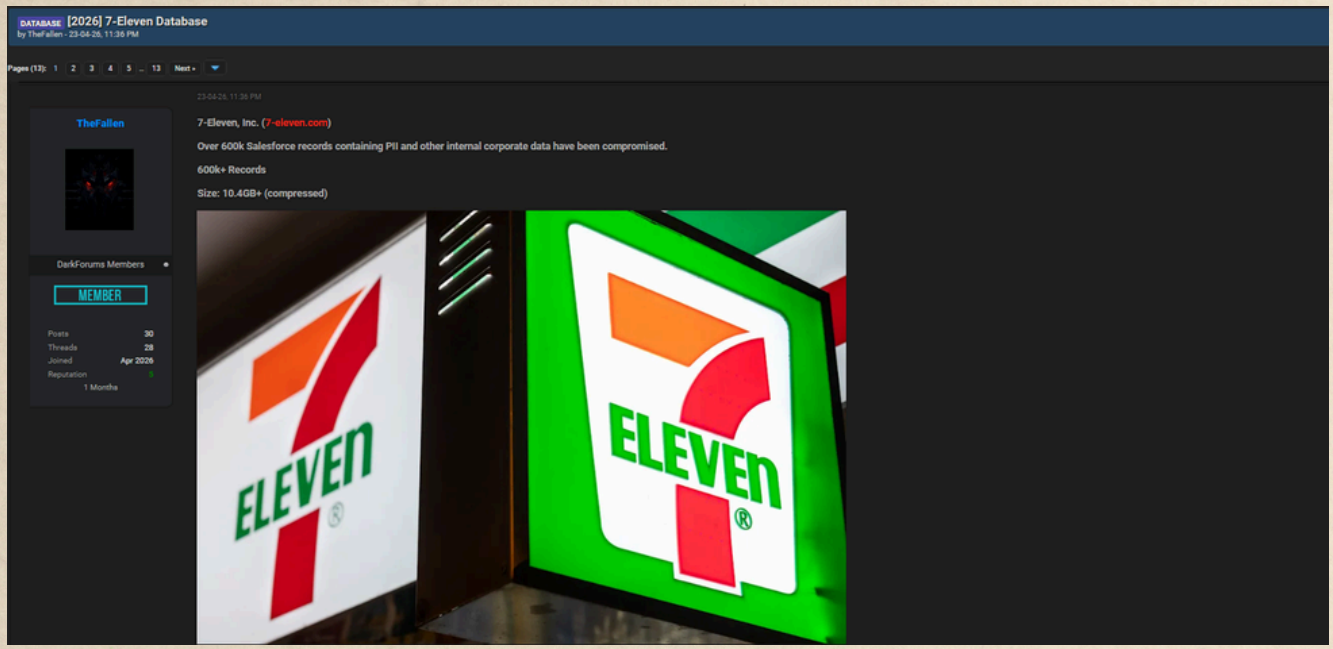
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 19 APR - 02 MAY 2026

7Eleven, Inc. Breach Incident

On April 23, 2026, a US company 7Eleven,Inc suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Retail / Convenience
Threat Actor : TheFallen
Data Sold: 10.4 GB



Key Highlights

- **Data Exposure:** Over 600K Salesforce records reportedly compromised, including PII and internal corporate data
- **Threat Actor:** Claimed by TheFallen on an underground cybercrime forum
- **Leak Details:** Database allegedly shared in compressed archive format totaling 10.4GB
- **Threat Level:** Significant risk of data misuse, unauthorized access, and reputational impact due to exposed corporate information

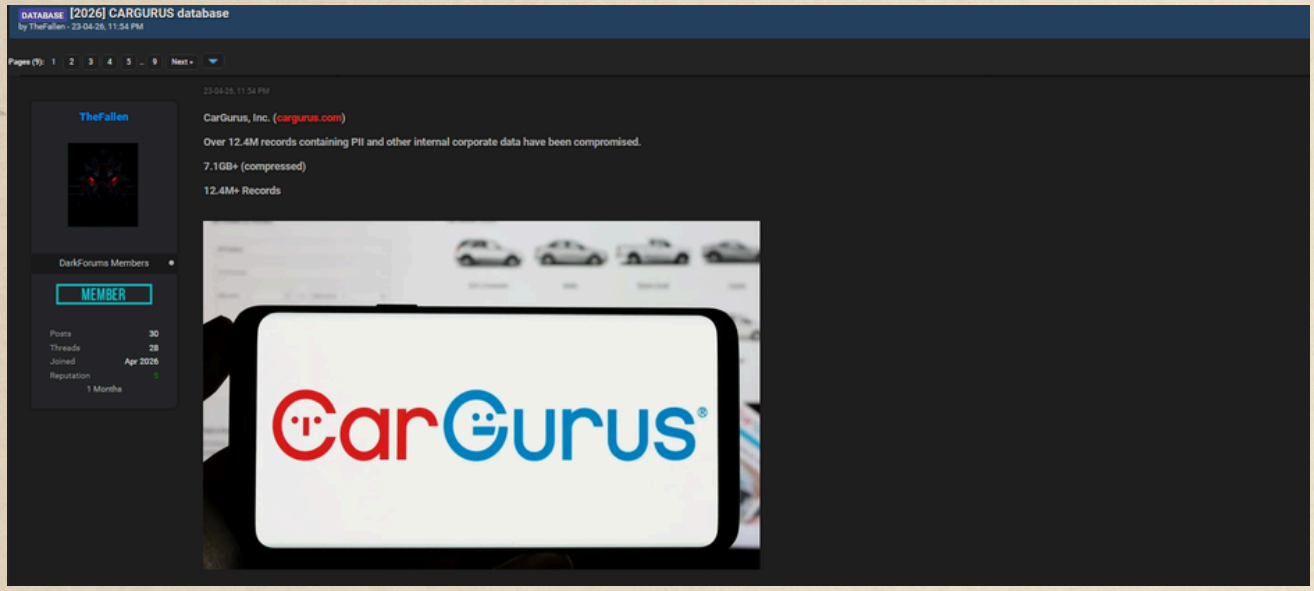
GLOBAL DATA BREACH REPORT

✳REPORTING PERIOD: 19 APR - 02 MAY 2026

CarGurus, Inc. Breach Incident

On April 23, 2026, a US company CarGurus, Inc. suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: **Automotive / E-commerce**
Threat Actor : **TheFallen**
Data Sold: **7.1 GB**



Key Highlights

- **Data Exposure:** Over 12.4M records reportedly compromised, containing PII and internal corporate data
- **Threat Actor:** Claimed by TheFallen on an underground cybercrime forum
- **Leak Details:** Alleged database archive shared in compressed format totaling 7.1GB
- **Threat Level:** Large-scale data exposure with risks of identity misuse, unauthorized access, and reputational damage

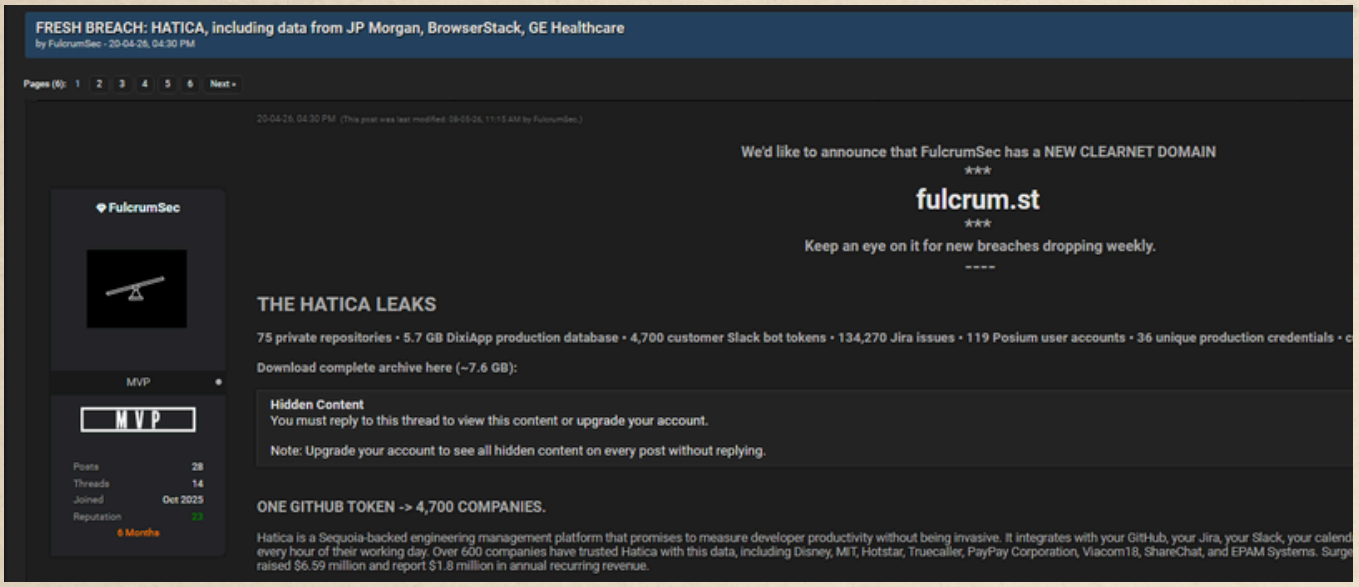
GLOBAL DATA BREACH REPORT

✱REPORTING PERIOD: 19 APR - 02 MAY 2026

Hatica, Inc Breach Incident

On April 20, 2026, a US company Hatica, Inc. suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Technology / Software as a Service (SaaS)
Threat Actor : FulcrumSec
Data Sold: 5.7 GB



Key Highlights

- **Data Exposure:** Leak allegedly includes 75 private repositories, 134K+ Jira issues, 4,700 customer Slack bot tokens, and plaintext application credentials
- **Affected Organizations:** Data reportedly linked to multiple enterprises including JP Morgan, BrowserStack, and GE Healthcare
- **Threat Actor:** Claimed by FulcrumSec on underground breach forum
- **Threat Level:** Critical exposure involving production credentials, tokens, and internal development assets with high risk of unauthorized access and supply-chain compromise

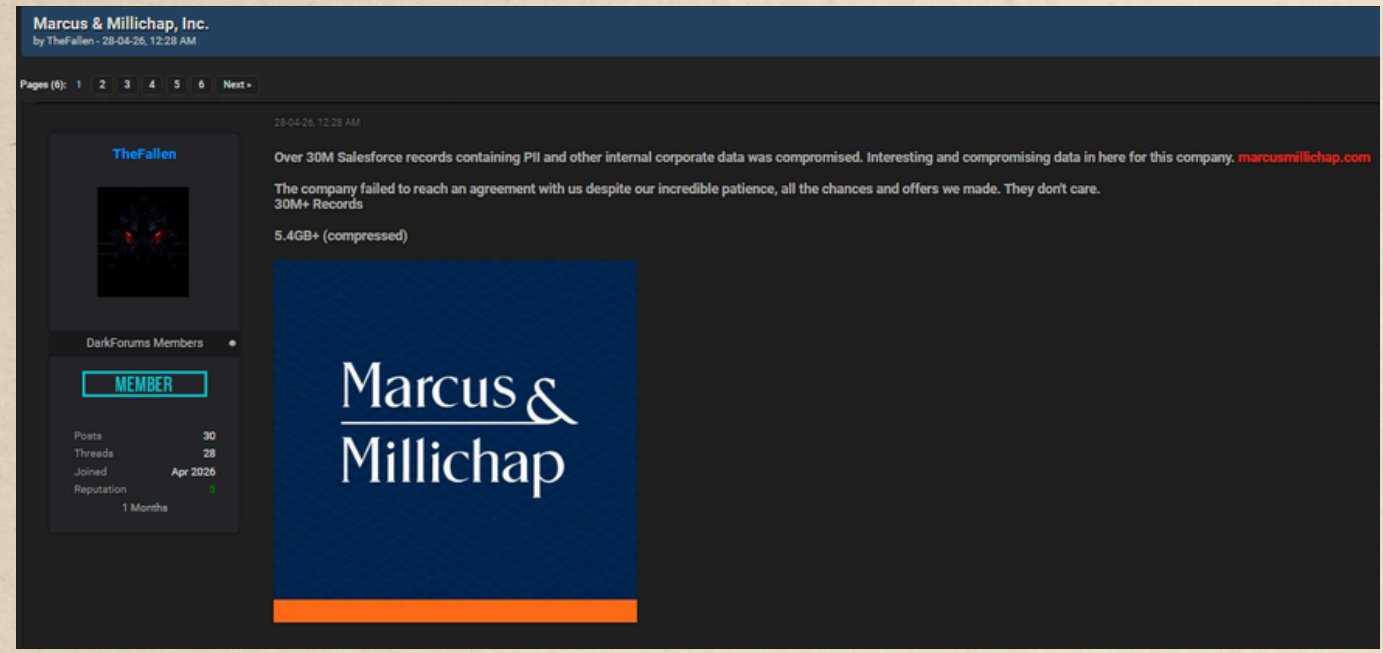
GLOBAL DATA BREACH REPORT

✳ REPORTING PERIOD: 19 APR - 02MAY 2026

Marcus & Millichap, Inc. Breach Incident

On April 28, 2026, a US company Marcus & Millichap, Inc. suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Real Estate Services
Threat Actor : TheFallen
Data Sold: 5.4 GB



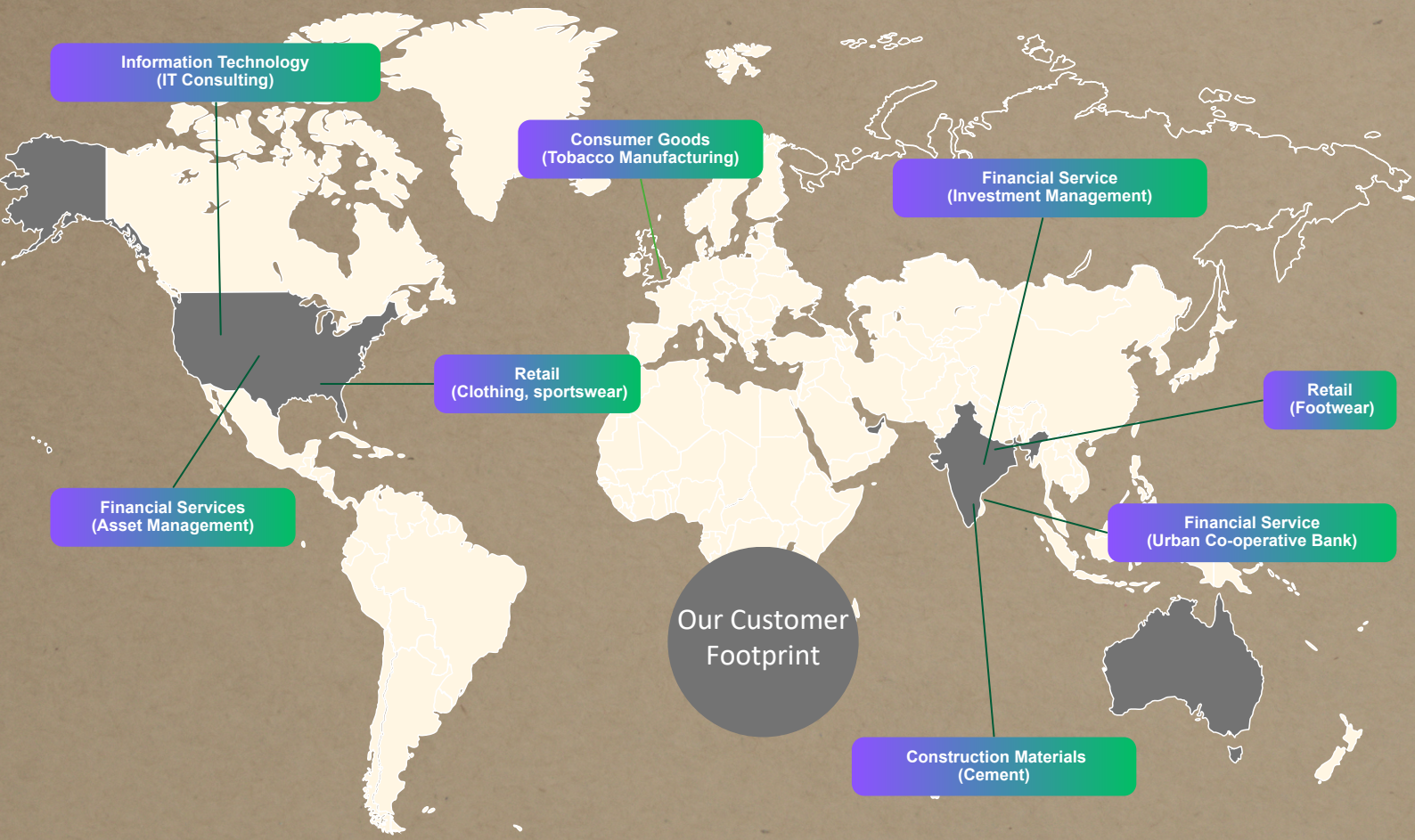
Key Highlights

- **Data Exposure:** Over 30M Salesforce records reportedly compromised, including PII and internal corporate data
- **Threat Actor:** Claimed by TheFallen on underground cybercrime forum
- **Threat Activity:** Threat actor alleges failed negotiations prior to disclosure of compromised data
- **Threat Level:** High-impact exposure with risks of identity theft, unauthorized access, and reputational damage due to large-scale corporate data leak

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