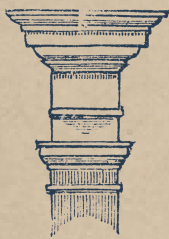


WEEKLY DIGEST

GLOBAL BREACHES & RANSOMWARE VICTIMS

REPORTING PERIOD: 07 JUNE – 13 JUNE 2026





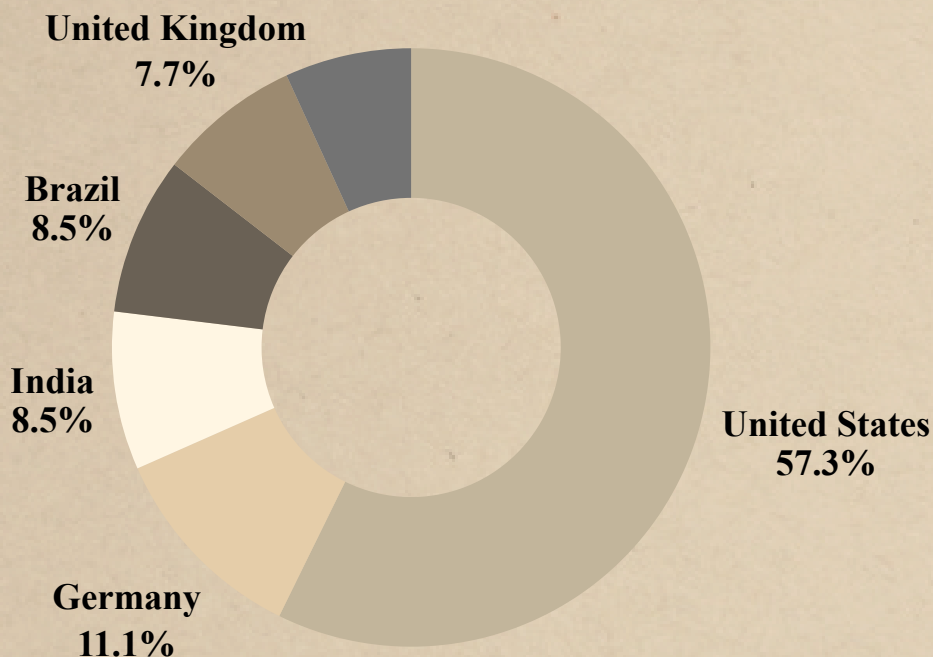
GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 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

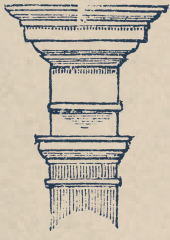


Key Highlights

- The majority of incidents were associated with ransomware and data extortion activity, underscoring the continued prevalence of financially motivated cyber threats.
- Threat groups such as **LockBit**, **Qilin**, **The Gentlemen**, and **DragonForce** were most frequently observed, indicating sustained and coordinated attack campaigns.

Most Targeted Sector: Manufacturing
Ransomware-linked breaches: 91.3 %

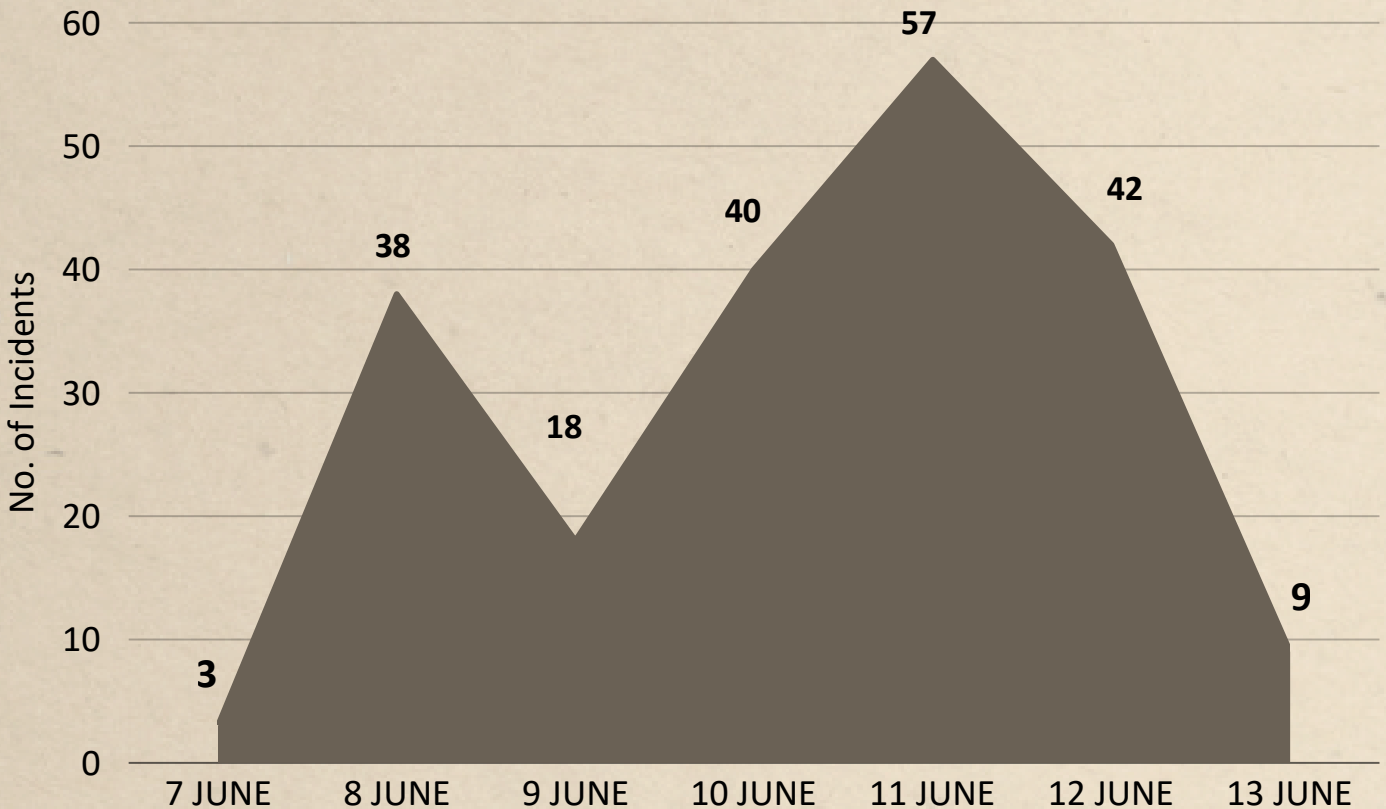
Total Breaches Observed: 207
Countries Affected: 48



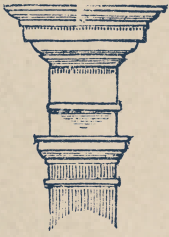
GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

Breach Over time



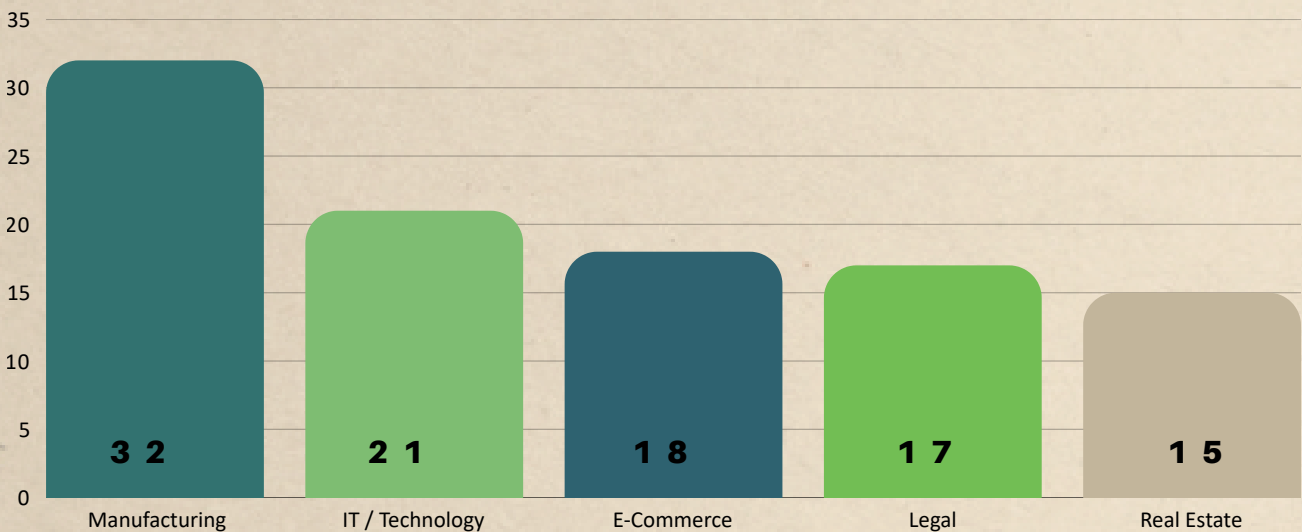
- Breach activity fluctuated throughout the period, with June 11, recording the highest spike at 57 reported incidents.
- A sharp rise was observed between June 9 and June 10, peaking at 40 incidents on June 10, indicating intensified disclosure or attack activity.
- June 07 reported the lowest number of incidents, with only 3 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: 07 JUNE - 13 JUNE 2026

Affected Sectors

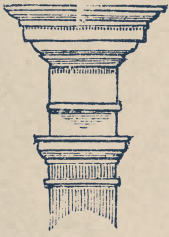


Industry Highlights

- Manufacturing & Engineering: **32+ incidents** (highest targeted sector)
- IT / Technology: **21+ incidents** (high exposure due to digital infrastructure)
- E-Commerce: **18+ incidents**
- Legal : **17+ incidents**
- Real Estate : **15+ incidents**



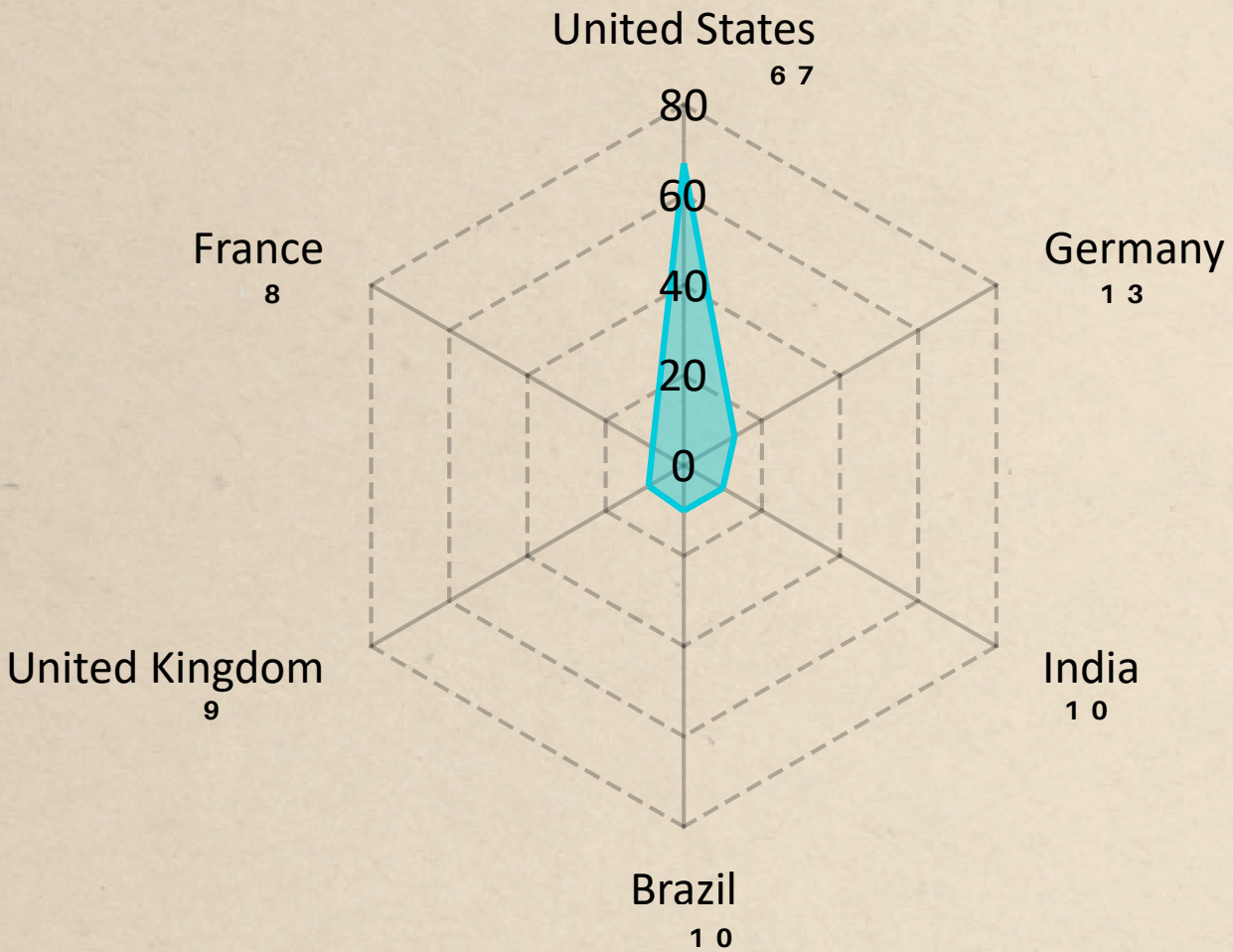
Industries Insight: Manufacturing continued to dominate incident volume, followed by technology, retail, finance, and construction sectors. These industries remain attractive targets due to their extensive digital infrastructure, supply chain dependencies, and access to sensitive operational and customer data.



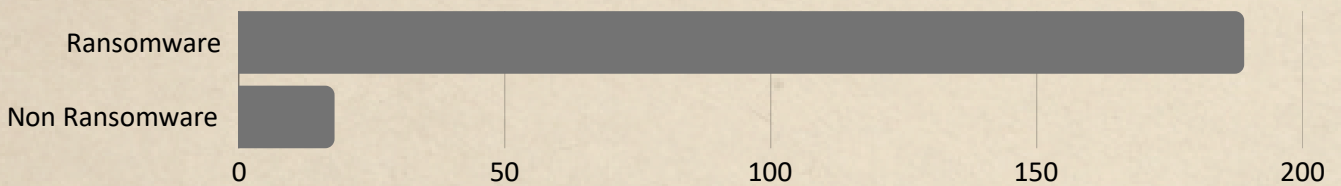
GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

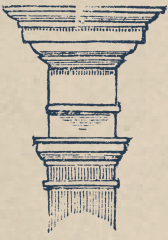
Affected Countries



Actor Distribution



Ransomware dominates the threat landscape with 189+ incidents, far outpacing 18 non-ransomware cases, making it the most prevalent and impactful attack type.



GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

Free S.A.S. Breach Incident

On June 11, 2026, a France company Free S.A.S. suffered a significant data breach during the week, involving potentially sensitive information.

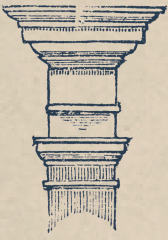
Company Sector: Telecommunications

Threat Actor : Cryptix

Data Sold: 43.5 GB

Key Highlights

- **Data Exposure:** Approx. 19M+ customer records reportedly leaked, including account identifiers, names, email addresses, phone numbers, postal addresses, and subscription information.
- **Threat Actor:** Linked to Cryptix.
- **Threat Activity:** Data was allegedly published on an underground forum as a 43.5 GB dataset, with sample records and dataset details provided.
- **Threat Level:** Critical, due to the large volume of customer PII exposed, creating risks of identity theft, phishing, account compromise, and large-scale fraud campaigns.



GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

Adobe Inc Breach Incident

On June 08, 2026, a USA company Adobe Inc suffered a significant data breach during the week, involving potentially sensitive information.

Company Sector: Technology

Threat Actor : Cryptix

Data Sold: 2.57 GB

DATABASE Adobe - 2.57GB Global Software Platform - User [150M+]
by Cryptix - 08-06-26, 06:20 PM

Pages (4): 1 2 3 4 Next »

08-08-26, 06:20 PM #1

Cryptix

Hello DarkForums Community,
Today I have uploaded an alleged Adobe user dataset from a global software and digital services platform.

Dataset Info:

- Domain: adobe.com
- Original File: Adobe
- Platform: Software / Digital Services
- Region: Global
- Total Records: 150M+ records
- Compressed File Size: 2.57 GB (2,766,039,188 bytes)

Reported Compromised Data:

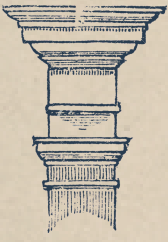
- User IDs
- Email Addresses
- Encrypted Passwords
- Password Hints

Banned

Posts 14
Threads 14
Joined Jun 2026
Reputation 2 Weeks

Key Highlights

- **Data Exposure:** Alleged leak of 150M+ Adobe user records from a global software and digital services platform.
- **Threat Actor:** Linked to Cryptix
- **Threat Activity :** User IDs, email addresses, encrypted passwords, and password hints.
- **Threat Level:** High – Exposed account data may enable credential-stuffing, phishing, and account takeover attempts.



GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

Apollo.io Breach Incident

On June 10, 2026, a USA company Apollo.io suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Sales Intelligence, B2B Lead Generation

Threat Actor : Thoseen1990

Data Sold: 1.92GB

Apollo.io - 1.92GB Global B2B Contact Database - [49M+ Records]
by Thoseen1990 · 10-06-26, 02:45 PM

10-06-26, 02:45 PM

Thoseen1990
Hello DarkForums Community,
Today I have uploaded the Apollo.io Records Dataset containing global professional and business contact information with approximately 49.19 million records.

Dataset Information:

- Source: Apollo.io
- Original File: apollo.io.v5
- Platform: B2B Contact Intelligence / Sales Intelligence Platform
- Region: Global
- Total Records: 49,189,288 lines
- Compressed File Size: 1.92 GB (2,069,704,298 bytes)

Compromised Data:

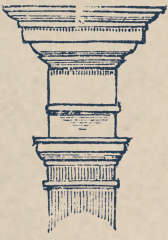
- Full Names
- Email Addresses
- Phone Numbers

DarkForums Members
MEMBER

Posts 2
Threads 2
Joined Jun 2026
Reputation 0
1 Weeks

Key Highlights

- **Data Exposure:** Alleged leak of 49.1M+ Apollo.io records containing global business and professional contact information.
- **Threat Actor:** Linked to Thoseen1990.
- **Threat Activity:** Dataset advertised and distributed on an underground forum, offering large-scale access to business contact intelligence data.
- **Threat Level:** Increased risk of phishing, business email compromise (BEC), spam campaigns, and targeted social engineering attacks.



GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

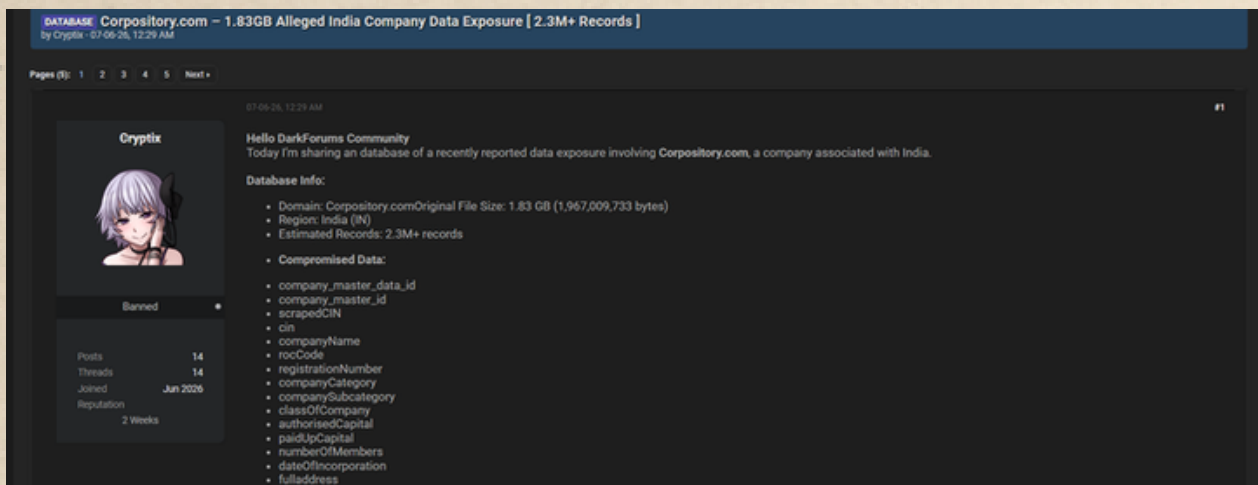
Corpository Breach Incident

On June 07, 2026, a Indian company Corpository suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Financial Technology

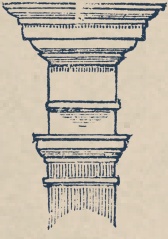
Threat Actor : Cryptix

Data Sold: 1.83 GB



Key Highlights

- **Data Exposure:** Alleged exposure of 2.3M+ Indian company records associated with Corpository.com.
- **Threat Activity:** Dataset advertised and shared on an underground forum, claiming access to extensive corporate registration and business intelligence data.
- **Threat Actor:** Linked to Cryptix.
- **Threat Level:** Medium–High – Could facilitate corporate reconnaissance, targeted phishing, business fraud, and supply-chain intelligence gathering.



GLOBAL DATA BREACH REPORT

* REPORTING PERIOD: 07 JUNE - 13 JUNE 2026

IMOVEQROO Breach Incident

On June 08, 2026, a Mexico company IMOVEQROO suffered a significant data breach during the week, involving potentially sensitive information..

Company Sector: Government / Public Infrastructure

Threat Actor : alecc157

Data Sold: 1.5 GB

DATABASE Leak - Licencias - 36.9K - Quintana Roo - Mexico
by alecc157 - 08-06-26, 03:48 AM

08-06-26, 03:48 AM

alecc157

DarkForums Members

MEMBER

Posts 2
Threads 2
Joined May 2026
Reputation 1 Months

Hacked by: Alecc157
SOCIEDAD PRIVADA 157

Hola comunidad de darkforums hoy les traigo un nuevo Leak sobre Licencias de Quintana roo (Municipio benito juarez) - (Mexico)
Este Leak contiene 36,999 Licencias en archivos .PDF Y en formato .HTML Con un Peso De 42.1GB
Las Licencias contienen: Datos Personales, Clave Castral, Telefonos, Direccion, Correos Y Datos De empresa.
Download: <https://gofile.io/d/b0xaBE>

Sample in json:

```
Code:
{
  "documento": {
    "formato": "FUMP",
    "expediente": 1,
    "tramite": {
      "tipo_tramite": "X",
      "tipo_movimiento": "X"
    },
    "licencia": {
      "numero": "",
      "clave_catastral": "501200200481500006",
      "licencia_alcohol": "",
      "giro_patente": "",
      "contribuyente": {
        "rfc": "PUN97002109CJ",
        "tipo_registro": "X",
        "es_matriz_o_sucursal": "X",
        "nombre": "Manuel Macouzet",
        "representante_legal": ""
      },
      "nombre_comercial": "Soul Bike Rental",
      "fecha_inicio_operaciones": "05/02/2019",
      "giro": {
        "descripcion": "Renta de bicicletas"
      },
      "ubicacion": {
        "supermanzana": "2A",
        "manzana": "56",
        "lote": "29",
        "numero_exterior": "34",
        "numero_interior": "499",
        "calle": "Av Carlos Nader",
        "localidad": "",
        "codigo_postal": "77500",
        "contacto": {
          "telefono": "5529660497",
          "email": "hola@soulbikerental.com"
        },
        "predio": {
          "es_propietario": "X",
          "documento_posesion": "Contrato de arrendamiento",
          "fecha_expiracion_posesion": {
            "dia": "05",
            "mes": "02",
            "año": "2019"
          },
          "operacion": {
            "superficie_m2": 45.65,
            "monto_inversion": 100.00,
            "empleados_hombres": 0,
            "empleados_mujeres": 0,
            "basura_kg": 1,
            "dias": "Lunes a Domingo",
            "banario": {
              "hora_inicio": "09",
              "minuto_inicio": "00",
              "hora_fin": "18",
              "minuto_fin": "30",
              "otro": "",
              "alcohol": {
                "dia": "",
                "hora_inicio": "00",
                "minuto_inicio": "00",
                "hora_fin": "00",
                "minuto_fin": "00"
              }
            }
          }
        }
      }
    }
  }
}
```

Key Highlights

- **Data Exposure:** Alleged leak of 36.9K business license records from Quintana Roo, Mexico, totaling approximately 42.1 GB of data.
- **Threat Actor:** Linked to Alecc157.
- **Threat Activity:** Dataset advertised on an underground forum with downloadable files and sample records provided as proof of access.
- **Threat Level:** High – Exposure could enable identity theft, targeted phishing, fraud, and unauthorized use of personal and business information.

About Castellum Labs

Based in Hyderabad, India with global customer base across India, US, Europe

Started by people with decades of product, services & deep tech experience

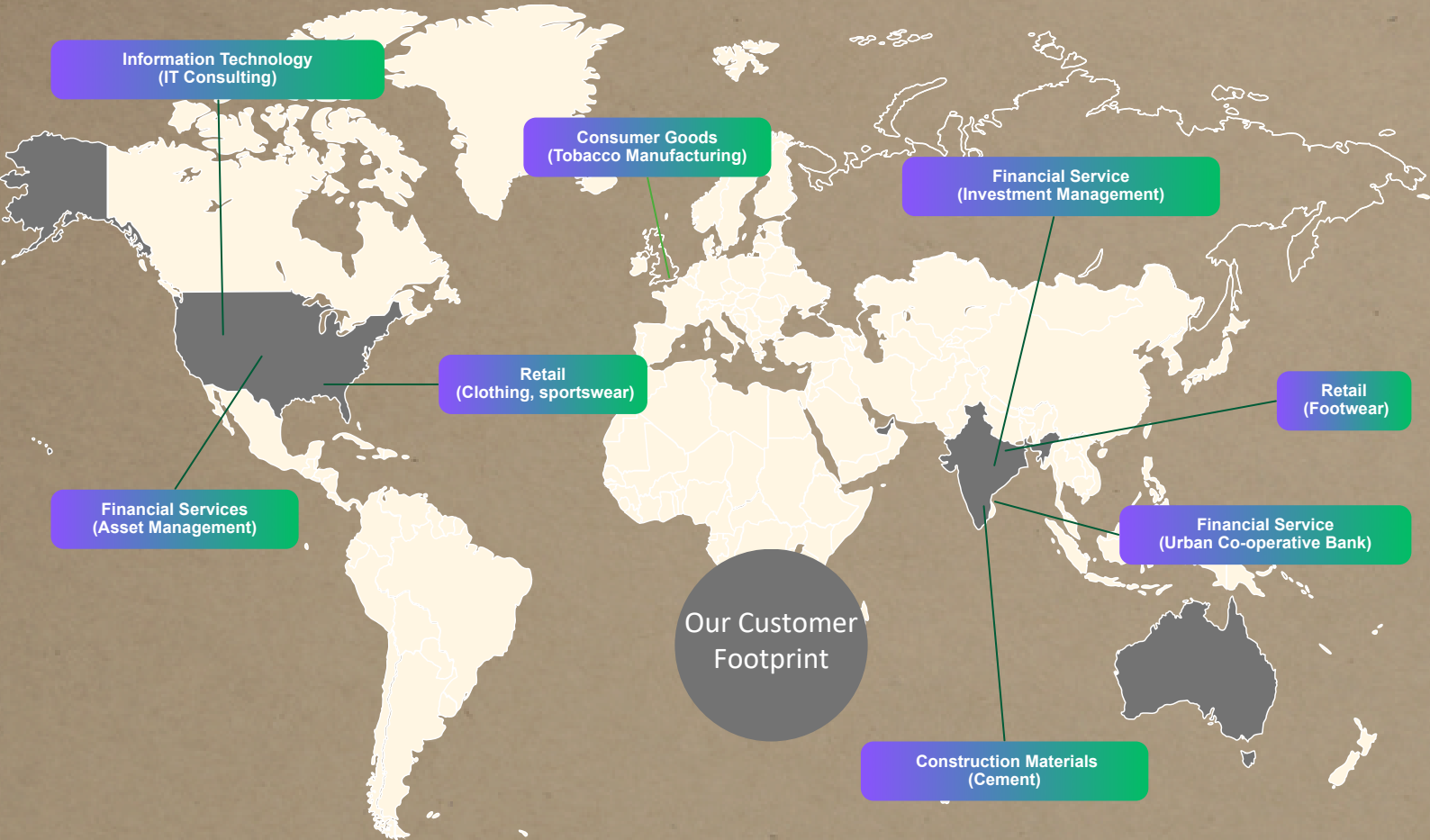
Value + Impact from Day One, No Installation & No Deployment

Services delivered by Global Cyber Capability Center using advance Platforms

Strong Handpicked Team of 50+ with (best of security talent globally)

Subscription & annual contract modeled services delivered globally

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 Vuln 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