

Monthly Business Review

December 1st to December 31st, 2025

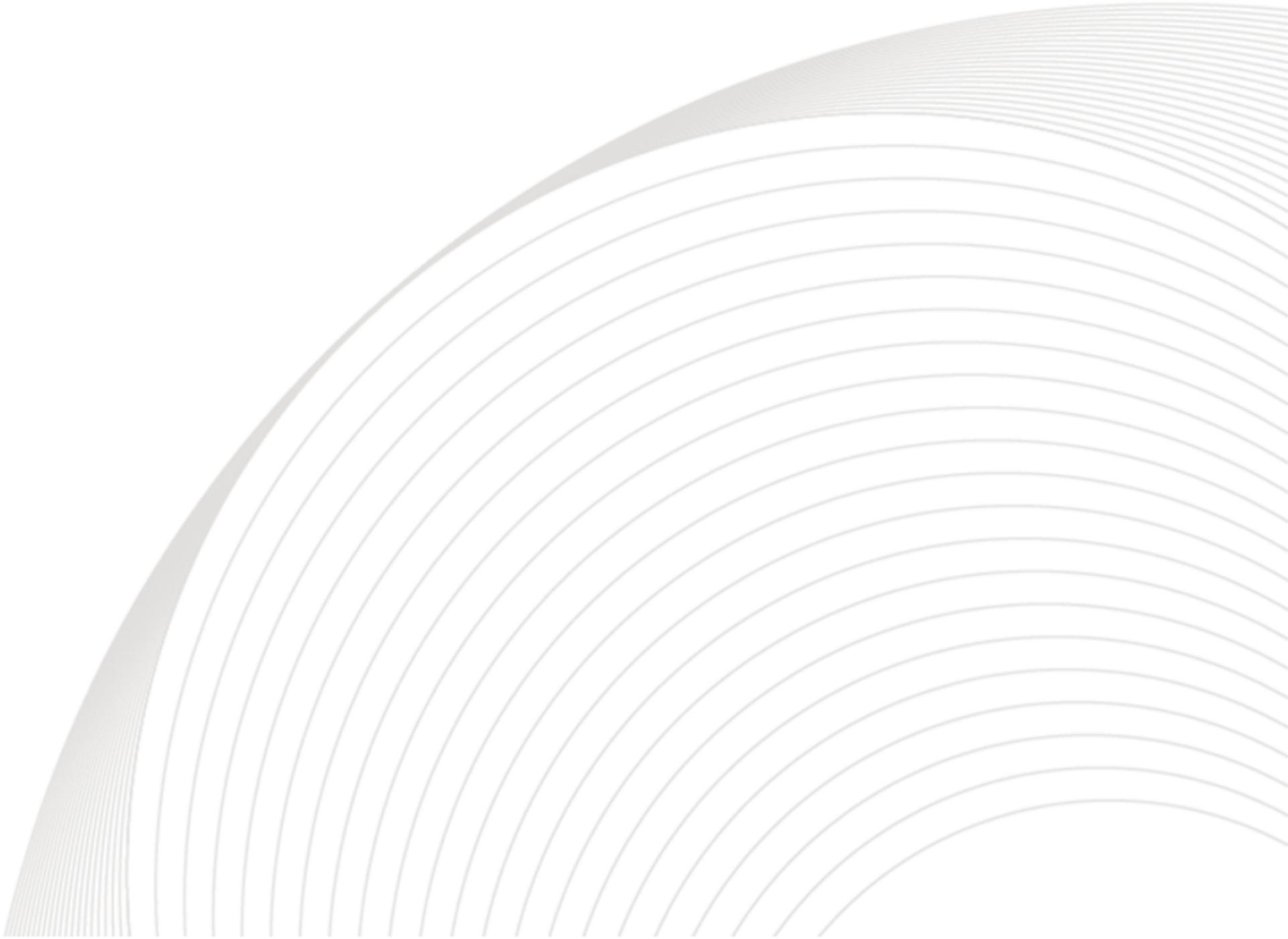


Table of Contents

- Introduction 3
- What is an Incident? 4
- What is Accidental Exposure? 4
- Report Content 5
- Statistics Charts 7
- Top Featured Breaches/ Incidents Detected 11

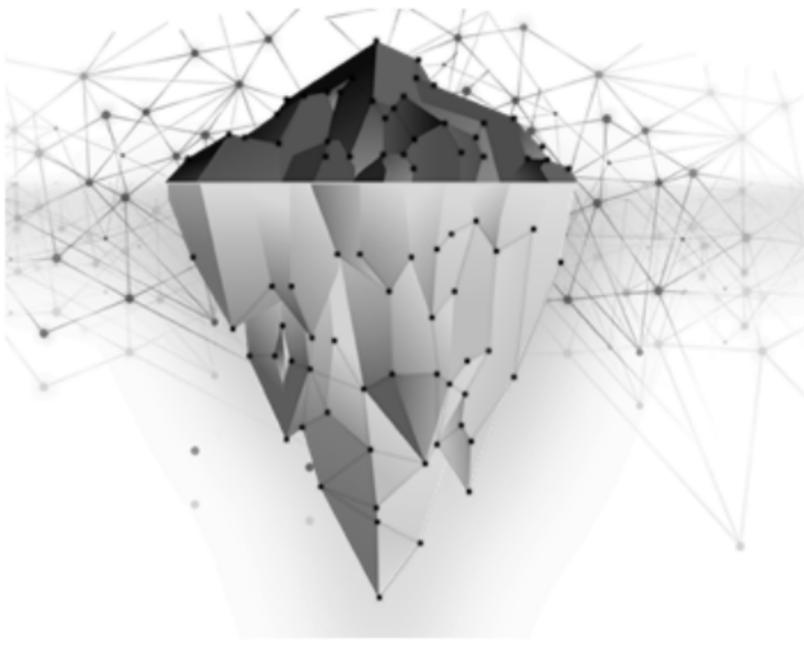
Disclaimer

The information in this report has been prepared to alert potentially affected parties of exposed data that may be publicly available using online resources. Constella Intelligence, Inc. does not make any representations, warranties or guarantees with respect to the completeness or accuracy of the reported exposures or any other information in this report.



Introduction

In the last few years, we have seen an increase in the number of incidents and data breaches. Hackers, organized crime, and nation sponsored attacks around the world have resulted in a surge of stolen data being sold in the black market. Billions of usernames, passwords, and terabytes of documents have been exposed in the deep and dark web. Constella Intelligence monitors the surface, social, deep and dark web detecting exposed identities and stolen data helping consumers and companies manage the risk.



230+ Billion

Processed Identity Records



What is an Accidental Exposure?

What is an Incident?

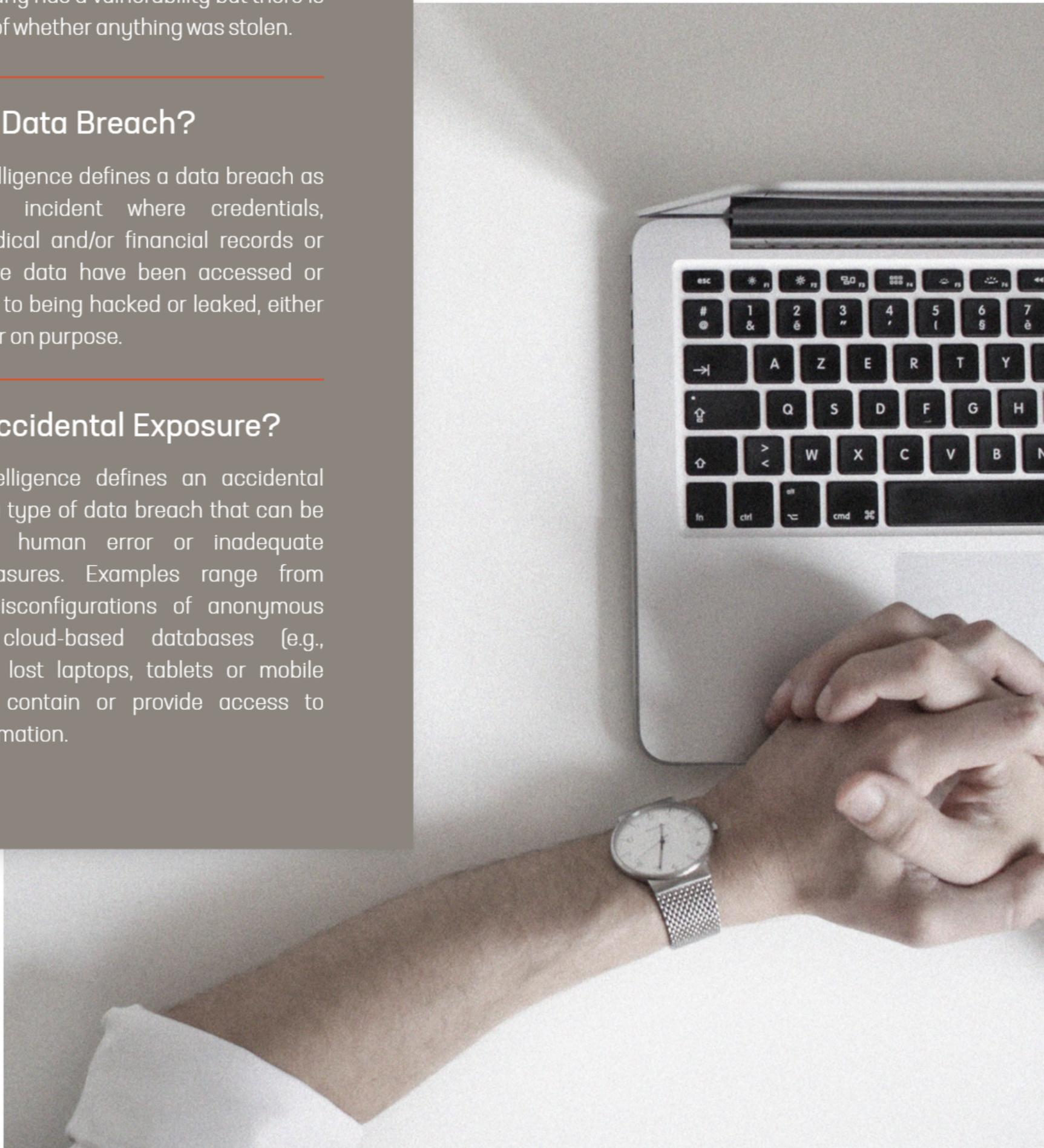
Constella Intelligence defines an incident as when a company has a vulnerability but there is confirmation of whether anything was stolen.

What is a Data Breach?

Constella Intelligence defines a data breach as a confirmed incident where credentials, personal, medical and/or financial records or other sensitive data have been accessed or disclosed due to being hacked or leaked, either accidentally or on purpose.

What is Accidental Exposure?

Constella Intelligence defines an accidental exposure as a type of data breach that can be attributed to human error or inadequate security measures. Examples range from default or misconfigurations of anonymous FTPs and cloud-based databases (e.g., MongoDB) to lost laptops, tablets or mobile phones that contain or provide access to sensitive information.



Report Content

All of the data breach information used in this report has been aggregated from the Constella Intelligence database between **December 1st to December 31st, 2025**. The following tables represent how the information has been classified depending on the data types.

All data has been extracted before the normalization and data accuracy analysis so the information shown in this report could vary. Each entry has been analyzed to determine the record types compromised.

Statistics

The total number of exposed identities in the month:

Raw Identity Records

Period	Num
Month	7,064,548,875

The total number of breaches found in the month:

New Breaches Found

Period	Num
Month	59,384

The total number of exposed identities after cleaning duplicates and fake data:

Cleansed Identities

Period	Num
Month	6,649,758,157

**Note: Due to the fact that combolists are created using parts from other breaches, they are not included in this table.*

Number of exposed identities by each type of breach (raw - not cleansed):

Identities Affected by Type of Breach

Type	Num
URL Logs	4,955,124,450
Leaked / Unknown	1,686,173,801
Combo Breaches	414,790,718
Hacked	8,459,906

Statistics Charts

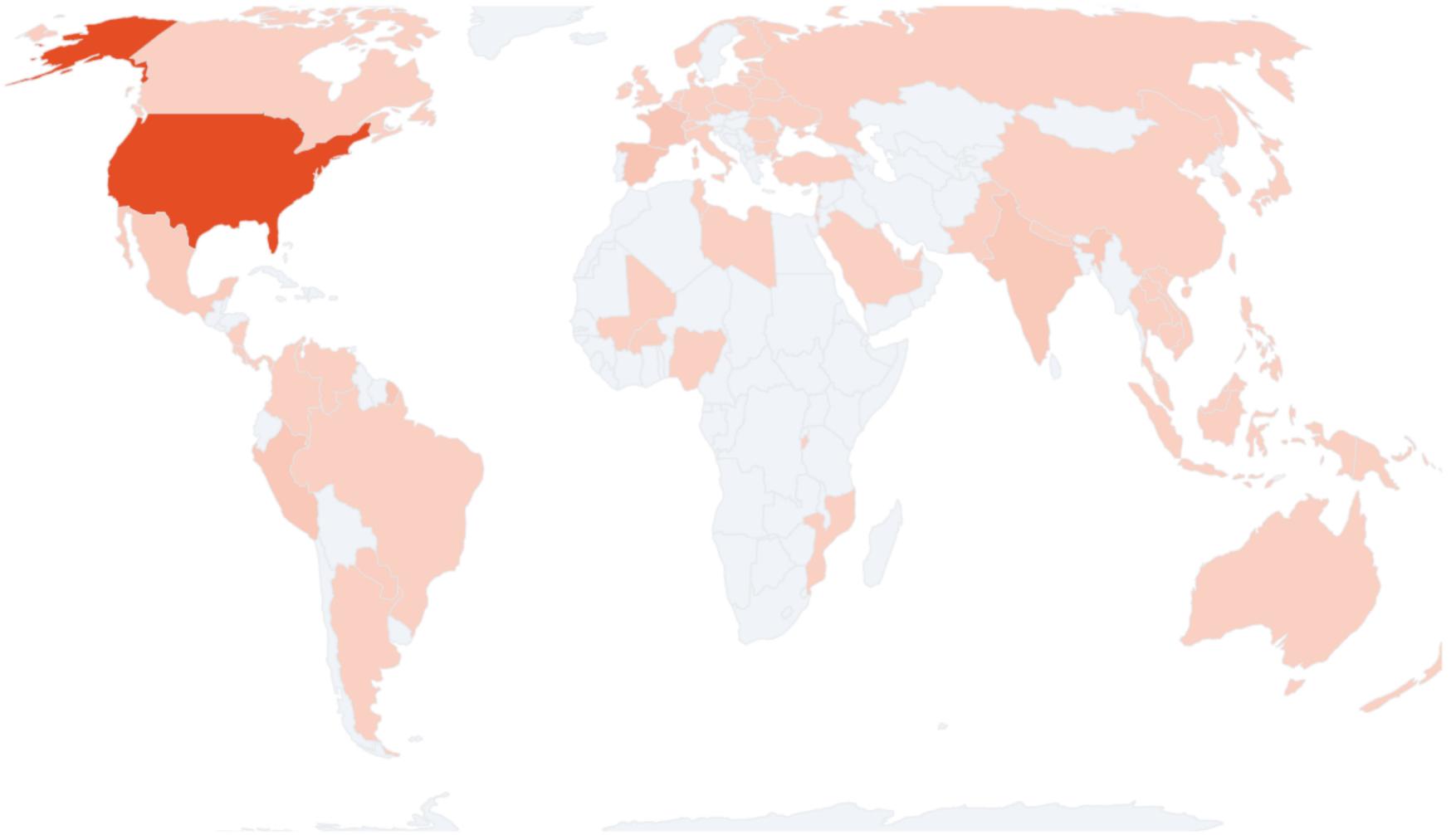
3.1 Monthly Breaches - Data Distribution (December 2025)

This chart shows the total number of records by exposed fields in the monthly breaches coming from analyzed identities:

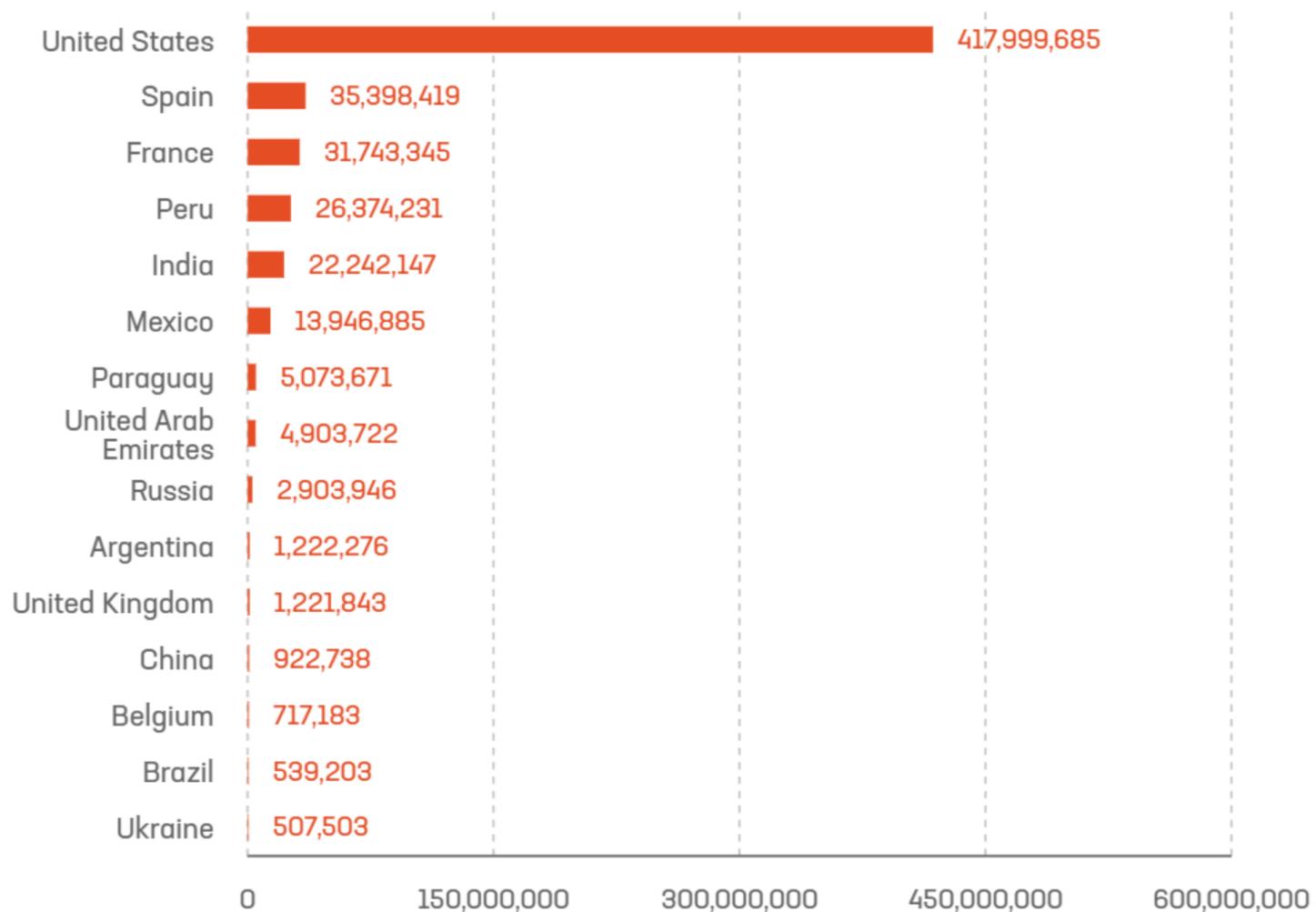


3.2 Geographic Distribution of Breaches (December 2025)

The following map represents the total number of records reported during **December 2025** geographically coming from analyzed identities:

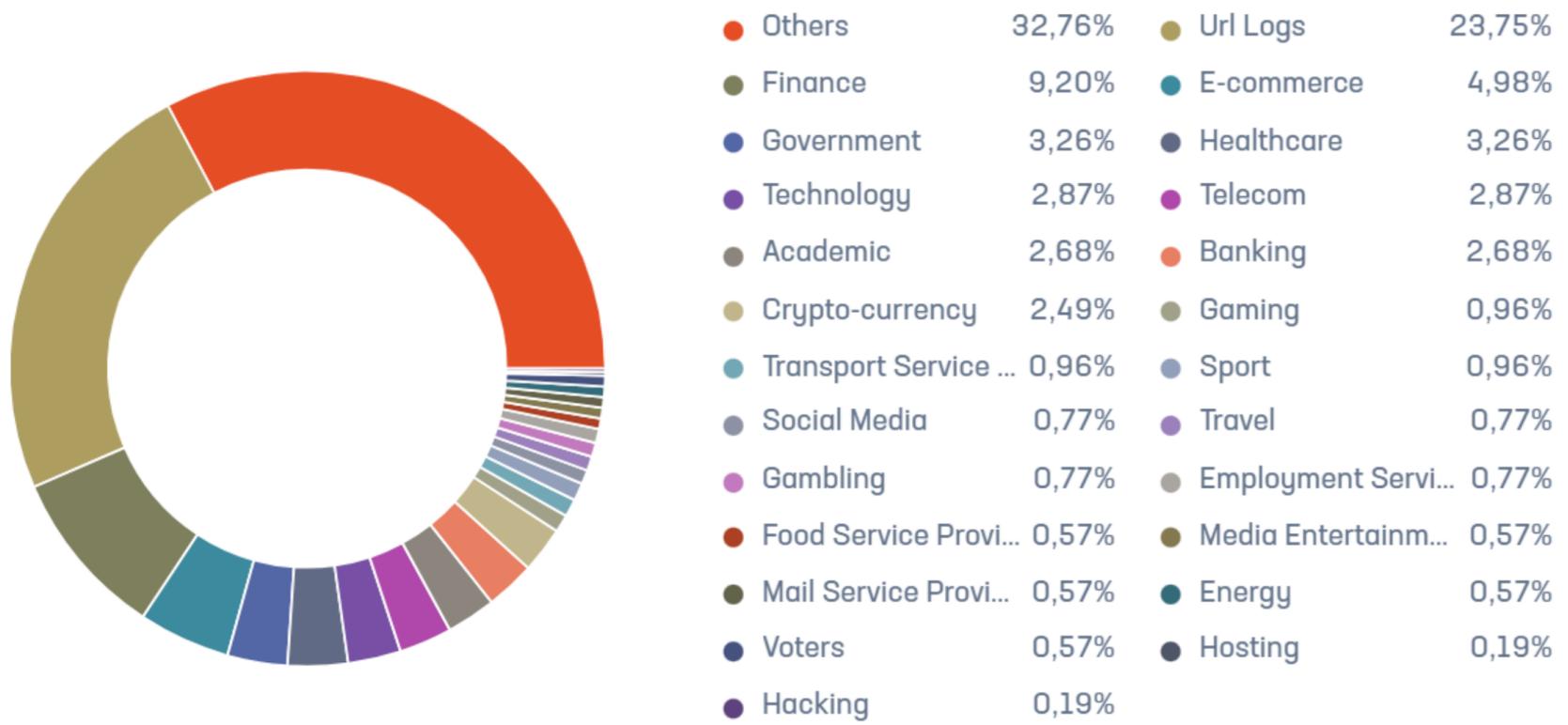


Geographic Location



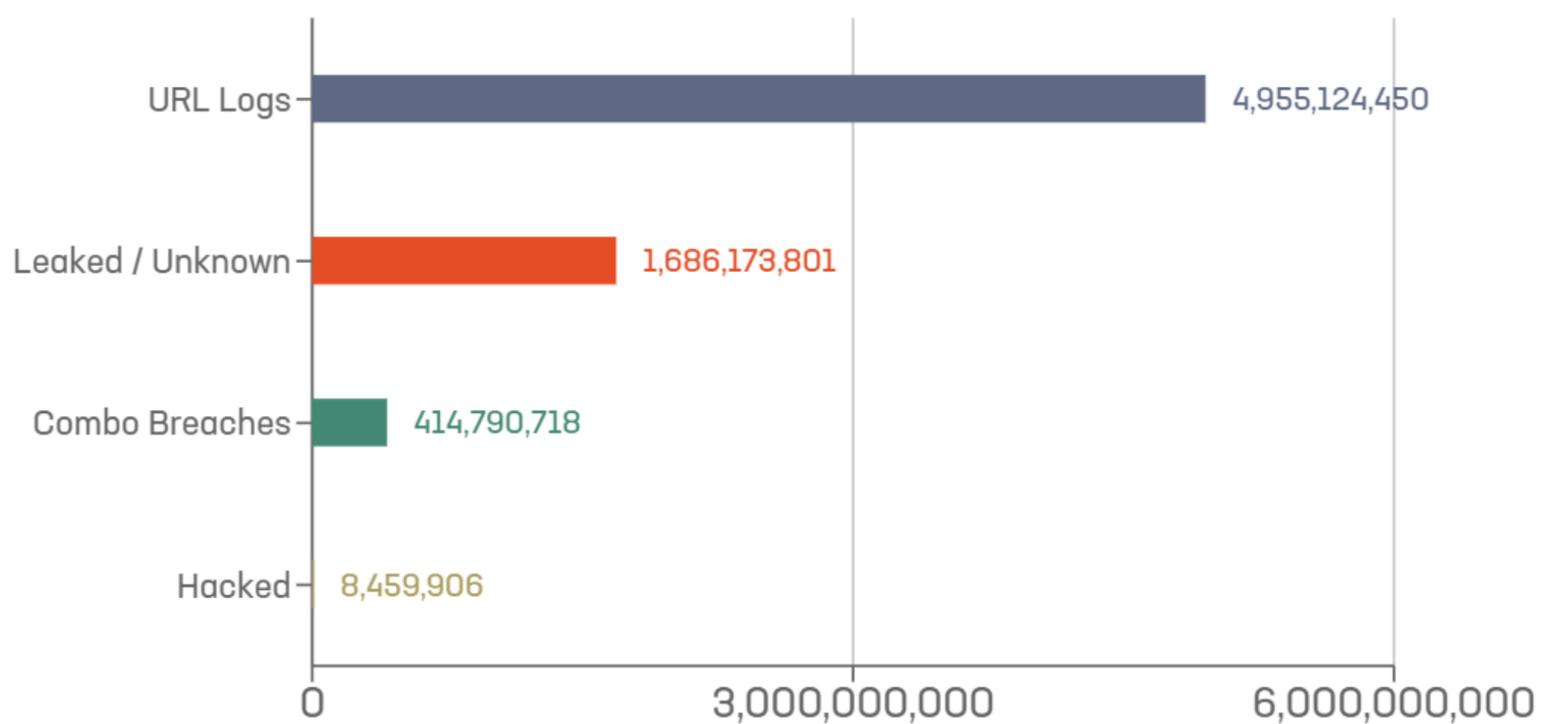
3.3 Distribution of incidents by Category (December 2025)

The following chart represents the percentage of breaches reported during **December 2025** by its category coming from analyzed identities:



3.4 Number of Identities Exposed by Type (December 2025)

The following chart represents the number of identities detected during December 2025 by its type:



3.5 Breach Distribution by Password Encryption Type (December 2025)

The following chart represents the percentage of breaches reported during **December 2025** by its type of encryption coming from analyzed identities:



● No Passwords	397 (56.71%)	● Plaintext	220 (31.43%)
● MD	17 (2.43%)	● Blowfish	10 (1.43%)
● bcrypt	10 (1.43%)	● Skein	8 (1.14%)
● HAVAL	5 (0.71%)	● PHPs	5 (0.71%)
● Joomla	5 (0.71%)	● WordPress	5 (0.71%)
● Unknown	5 (0.71%)	● Tiger	4 (0.57%)
● SHA	2 (0.29%)	● DNSSEC	2 (0.29%)
● MySQL	2 (0.29%)	● SHA	2 (0.29%)
● Drupal	1 (0.14%)		

Top Featured Breaches/ Incidents Detected

The top incidents reported in the month of December 2025 are:

Top Breaches from December 1st to December 31st, 2025

Breach Name	Description
autosur.fr	The site autosur.fr has been reported to possibly have suffered a data exposure that could include 5,790,401 names, surnames, addresses, zip codes, cities, phones, and emails. The possible exposure would have happened in March 2025 although it was reported in December 2025.
zeelabpharmacy.com	The site zeelabpharmacy.com has been reported to possibly have suffered a data exposure that could include 794,081 names, emails, phones, addresses, cities, states, surnames, usernames, companies, zip codes, and passwords. The possible exposure would have happened in September 2025 although it was reported in December 2025.
propostuplenie.ru	The site propostuplenie.ru has been reported to possibly have suffered a data exposure that could include 521,532 emails, passwords, usernames, phones, and cities. The possible exposure would have happened in November 2025 although it was reported in December 2025.
apoia.se	The site apoia.se has been reported to possibly have suffered a data exposure that could include 453,403 names, surnames, emails, zip codes, addresses, cities, and states. The possible exposure was reported in December 2025.
codestepbystep.com	The site codestepbystep.com has been reported to possibly have suffered a data exposure that could include 206,404 emails, names, surnames, and usernames. The possible exposure would have happened in November 2025 although it was reported in December 2025.

About Constella Intelligence

Constella Intelligence is a global leader in Digital Risk Protection, safeguarding 30M+ global users at some of the world's largest organizations, including 5 of the top 10 US banks. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your people, your brand, and your data - at scale.

Constella is powered by the most extensive breach and social data collection on the planet from the surface, deep, and dark web.

- Over 100B attributes and 45B curated identity records
- Spanning 125 countries and 53 languages.

Why Constella

OUR TEAM

We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify threats and reduce risks emerging from social media, the surface, deep, and dark web.

OUR DIFFERENCE

Our unique technology empowers advanced analysis of the entire risk surface for real time visibility of external threats protecting organizations, their employees, and their critical assets. Because the best way to overcome future digital threats is by facing them today.



© Constella Intelligence. All rights reserved.
Constella Intelligence and the Constella Intelligence logo are registered trademarks of Constella Intelligence.
Other names may be trademarks of their respective owners

www.constella.ai

 [constella/](https://www.linkedin.com/company/constella/)