Constella

Monthly Business Review

January 1st to January 31st, 2026

Date_February 2026

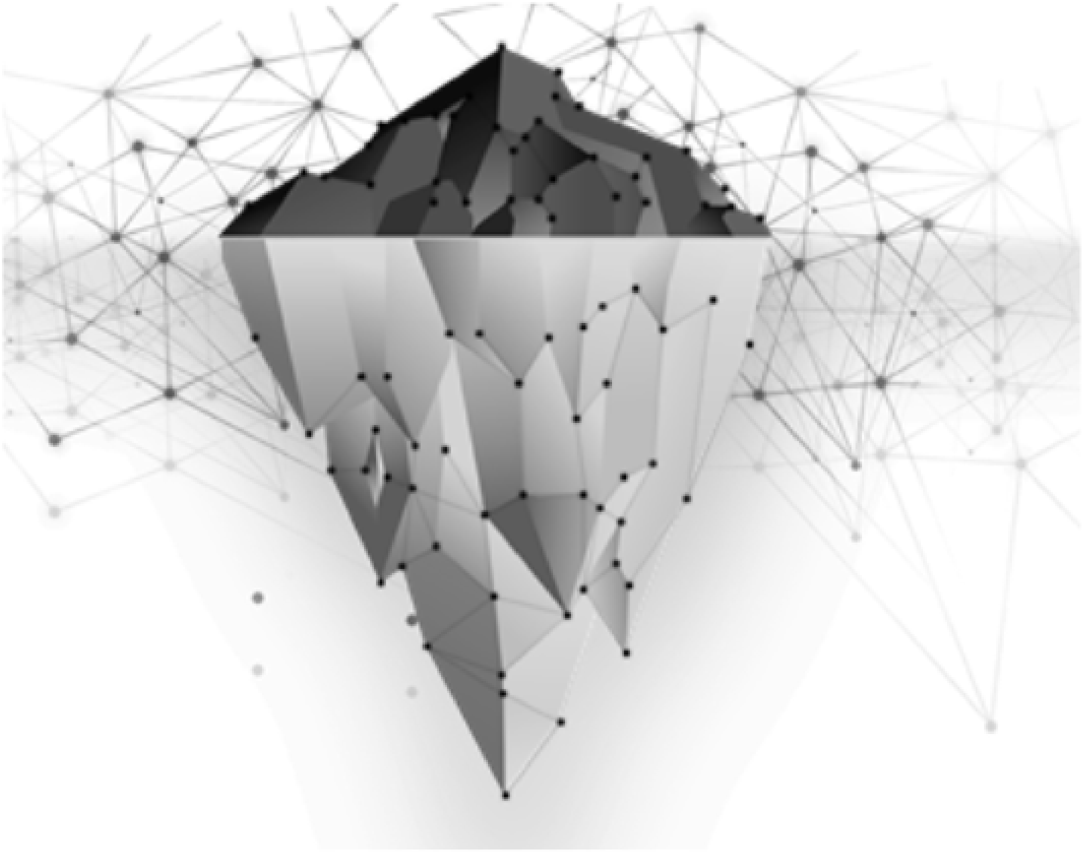
Table of Contents

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

>1.1 Trillion
Processed Assets

320+ Million
Alerts Triggered

500+ Million
Assets Monitored

53+
Languages for Alerts

What is an Accidental Exposure?

What is an Incident?

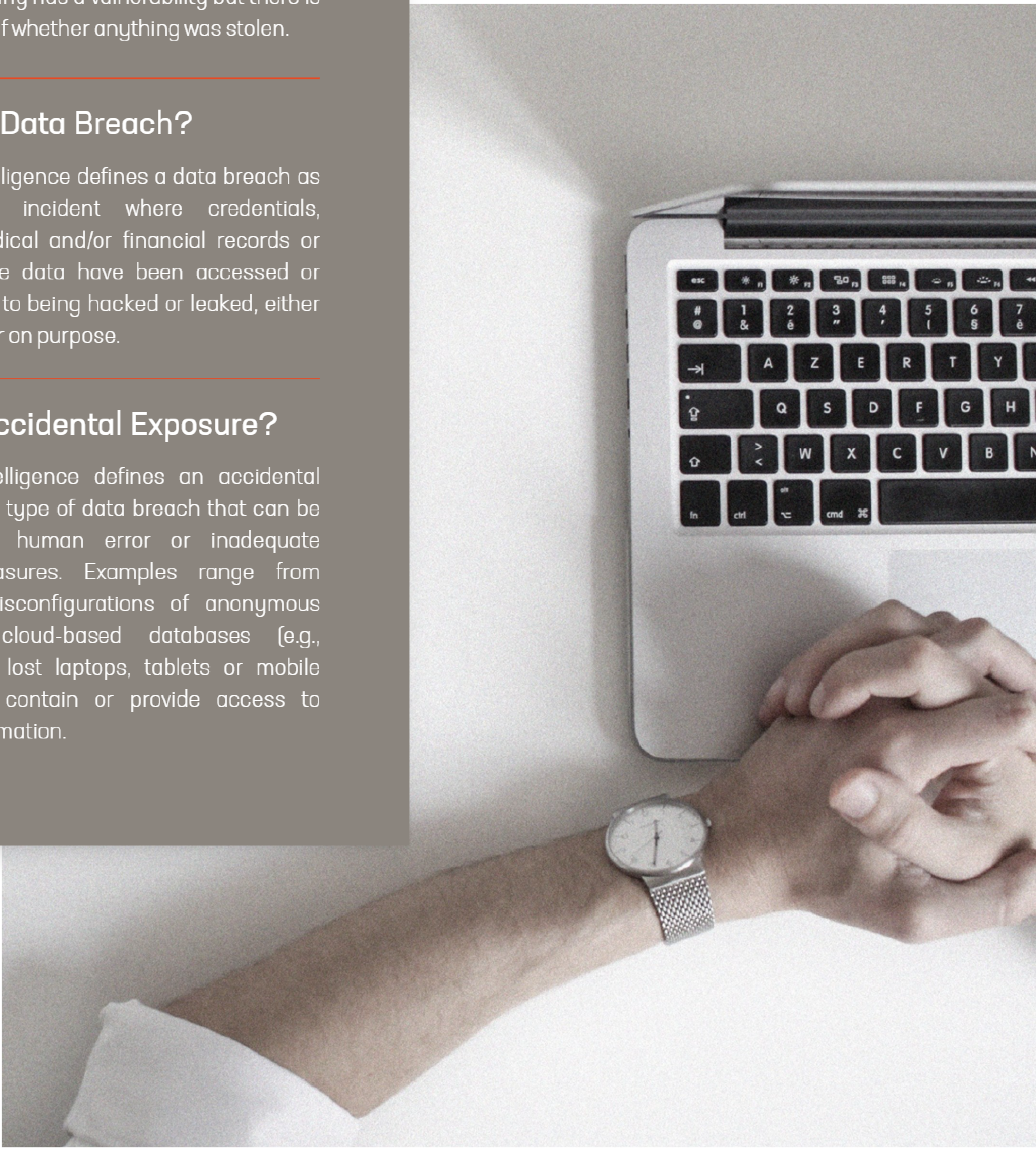
Constella Intelligence defines an incident as when a company has a vulnerability but there is confirmation of whether anything was stolen.

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 **January 1st to January 31st, 2026.** 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	12,623,191,955

The total number of breaches found in the month:

New Breaches Found

Period	Num
Month	27,177

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

Cleansed Identities

Period	Num
Month	12,398,604,356

**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	11,690,590,641
Leaked / Unknown	639,324,848
Combo Breaches	224,587,599
Hacked	68,688,867

Statistics Charts

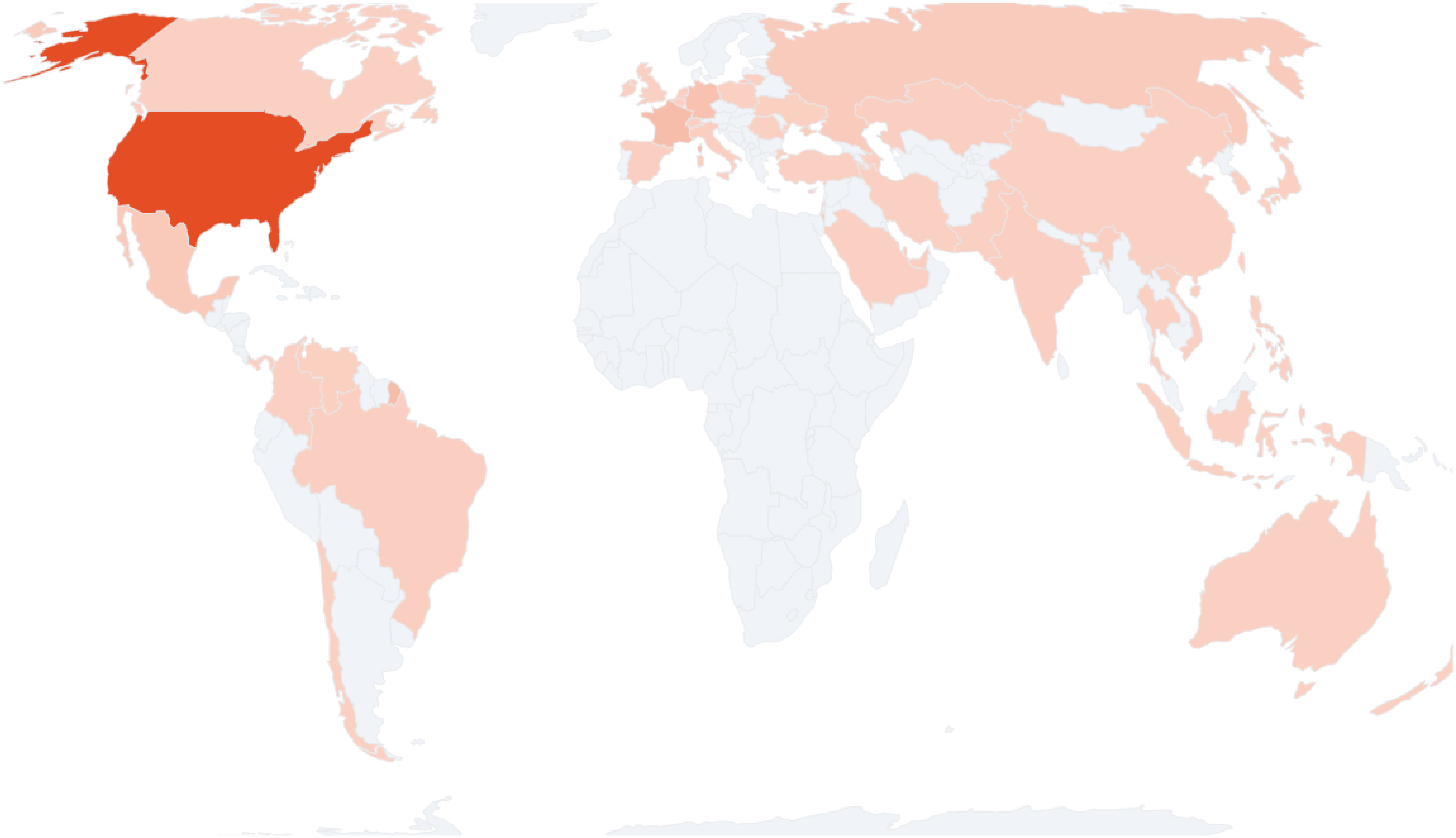
3.1 Monthly Breaches - Data Distribution (January 2026)

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

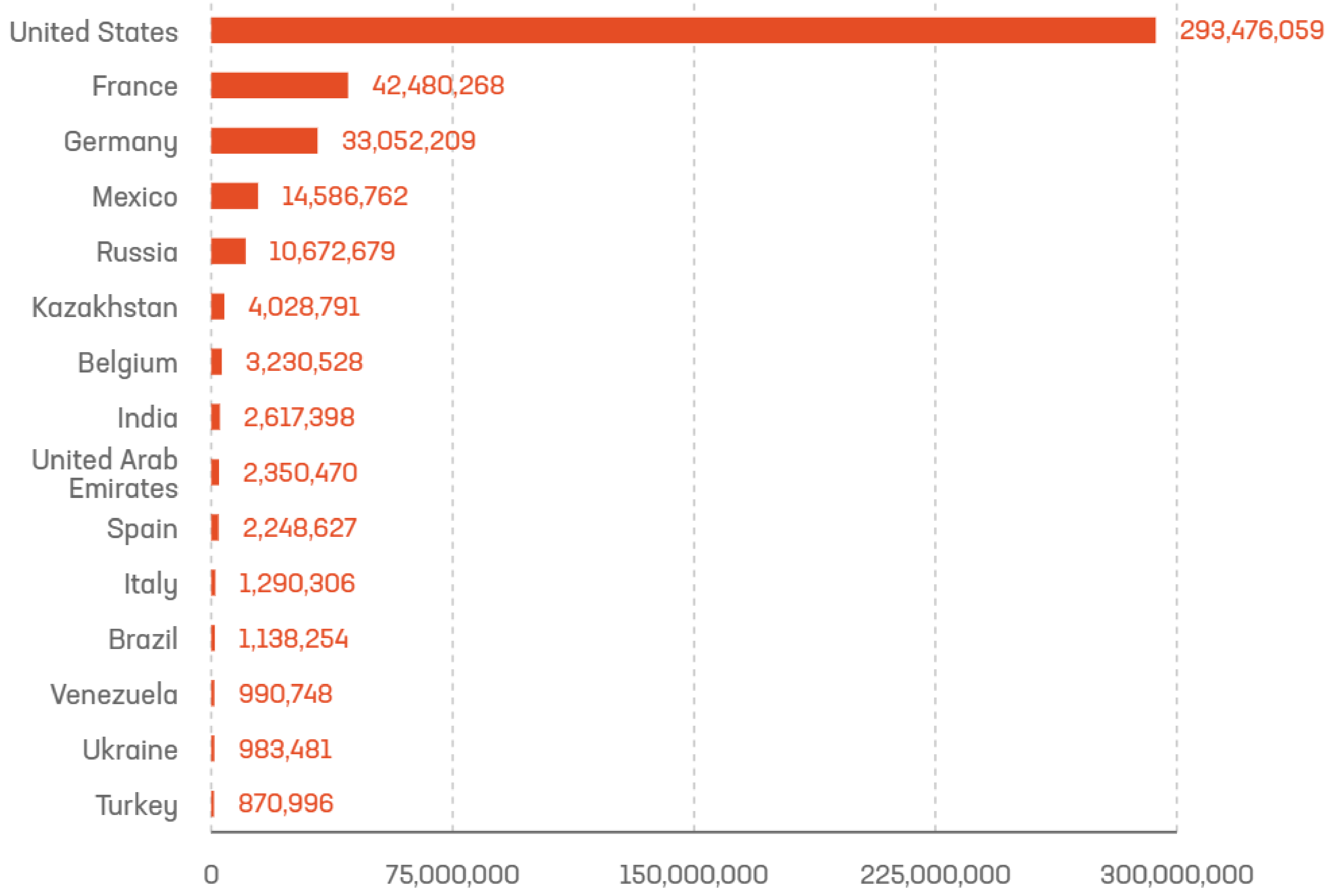
788,770,517	Email
225,574,362	Name
8,292,299	IP Address
133,319,258	Birthdate
1,081,297	Bank Account
533,893,003	Password
476,191,454	Username
177,016,779	Geographic Location
157,210,453	Phone number
349,114	SSN

3.2 Geographic Distribution of Breaches (January 2026)

The following map represents the total number of records reported during **January 2026** geographically coming from analyzed identities:

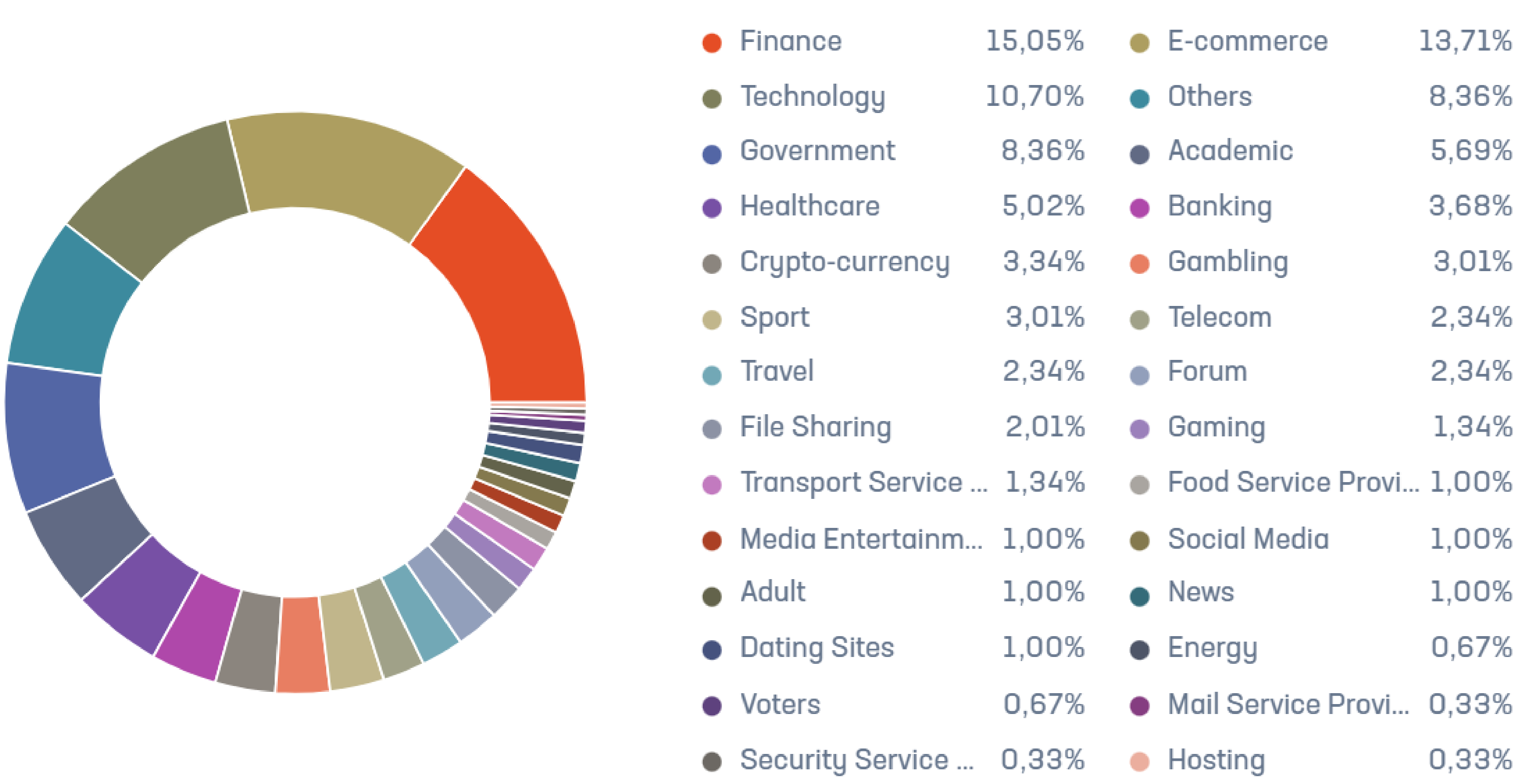


Geographic Location



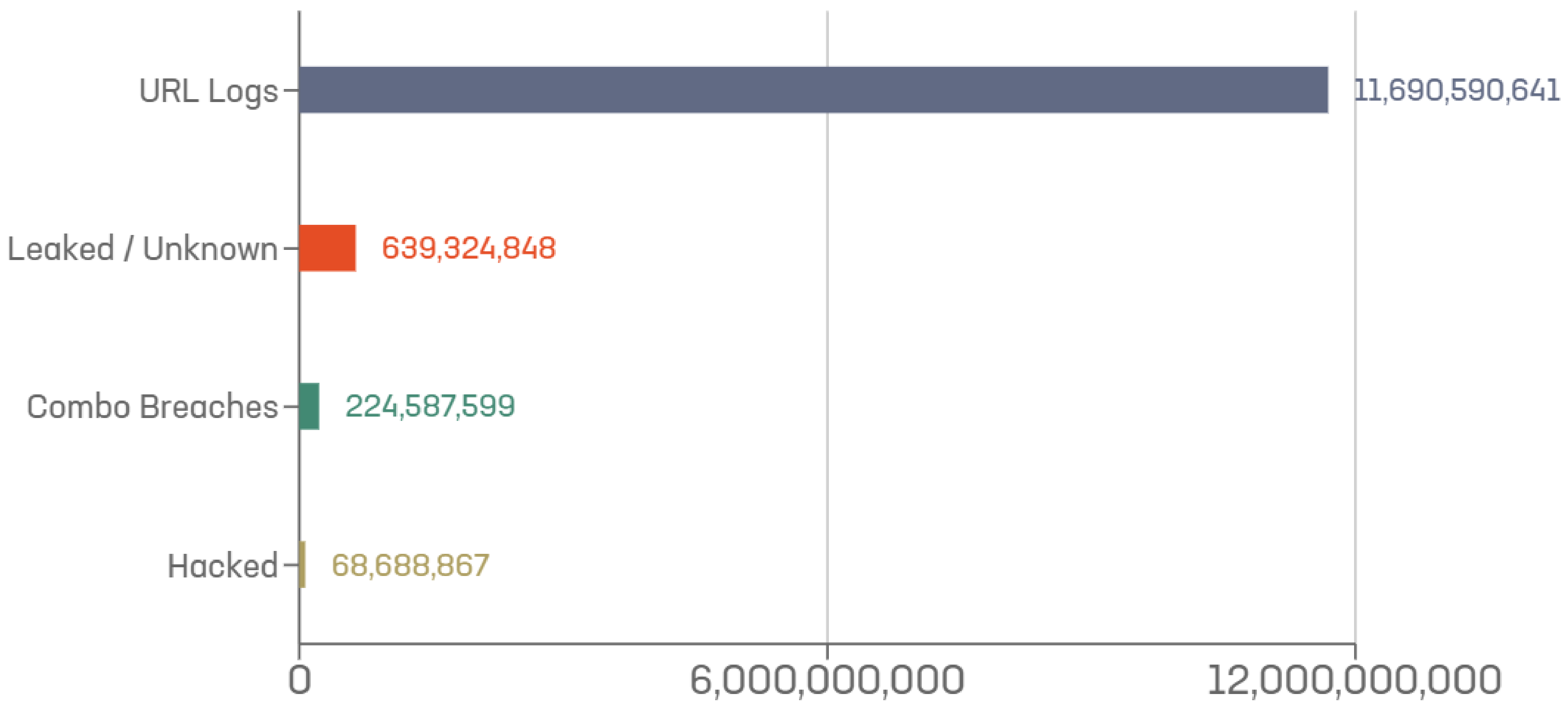
3.3 Distribution of incidents by Category (January 2026)

The following chart represents the percentage of breaches reported during **January 2026** by its category coming from analyzed identities:



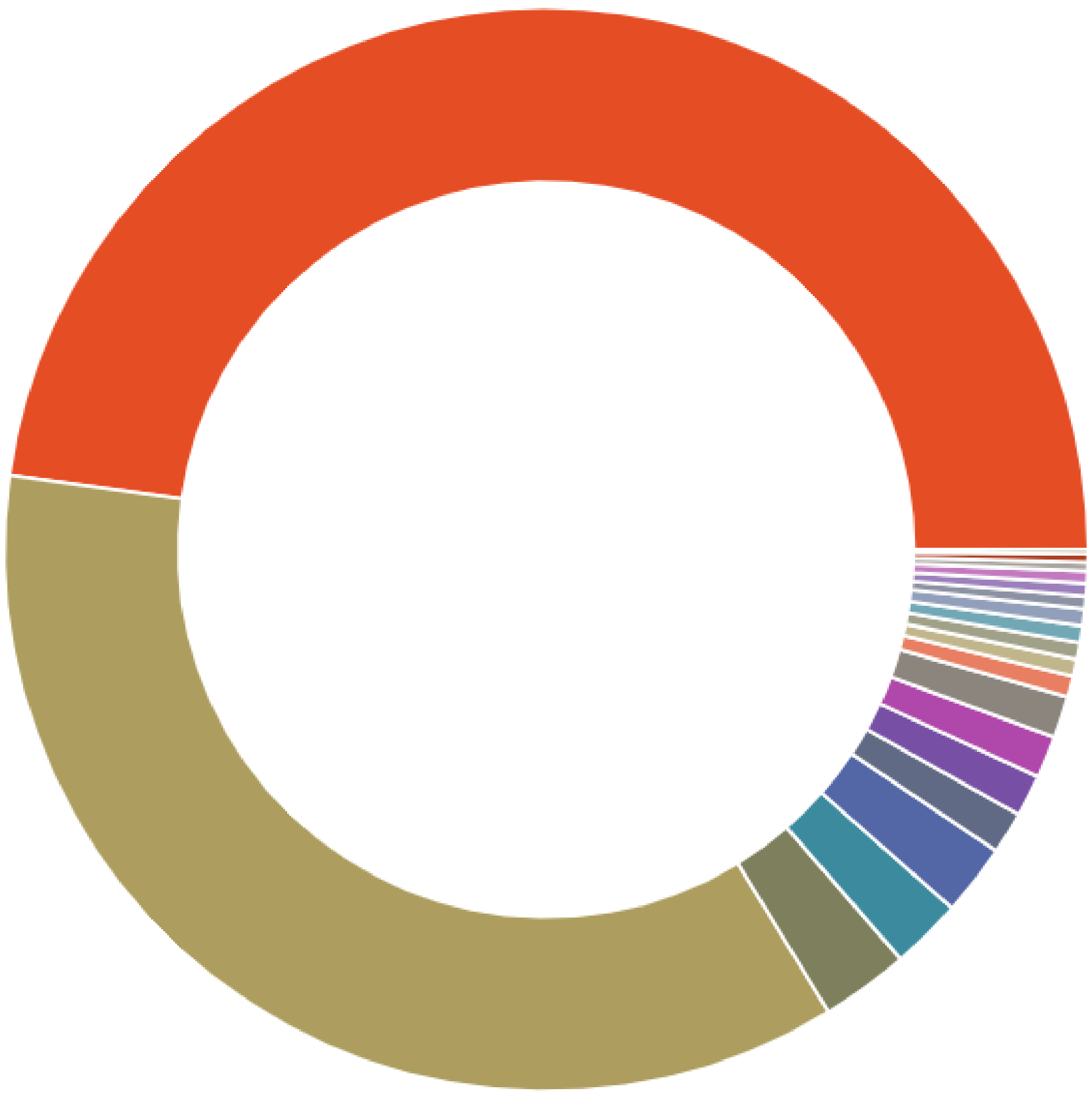
3.4 Number of Identities Exposed by Type (January 2026)

The following chart represents the number of identities detected during January 2026 by its type:



3.5 Breach Distribution by Password Encryption Type (January 2026)

The following chart represents the percentage of breaches reported during **January 2026** by its type of encryption coming from analyzed identities:



● Plaintext	382 (47.81%)	● No Passwords	287 (35.92%)
● MD	21 (2.63%)	● Blowfish	17 (2.13%)
● bcrypt	17 (2.13%)	● SHA	10 (1.25%)
● Skein	10 (1.25%)	● MySQL	10 (1.25%)
● SHA	10 (1.25%)	● Tiger	5 (0.63%)
● HAVAL	4 (0.50%)	● Snefru	4 (0.50%)
● Radmin	4 (0.50%)	● Unknown	4 (0.50%)
● DNSSEC	3 (0.38%)	● PHPs	3 (0.38%)
● Joomla	3 (0.38%)	● NTLM	2 (0.25%)
● WordPress	2 (0.25%)	● Salsa	1 (0.13%)

Top Featured Breaches/ Incidents Detected

The top incidents reported in the month of January 2026 are:

Top Breaches from January 1st to January 31st, 2026

Breach Name	Description
soundcloud.com	The site soundcloud.com has been reported to have suffered a data exposure that could include 29,892,439 names, surnames, cities, and emails. The exposure would have happened in December 2025 although it was reported in January 2026.
colisprive.fr	The site colisprive.fr has been reported to have suffered a data exposure that could include 22,526,525 surnames, names, phones, emails, and addresses. The exposure would have happened in November 2025 although it was reported in January 2026.
daryn.online	The site daryn.online has been reported to possibly have suffered a data exposure that could include 4,016,754 names, surnames, phones, emails, birthdates, and addresses. The possible exposure would have happened in January 2023 although it was reported in January 2026.
rezeptwelt.de	The site rezeptwelt.de has been reported to have suffered a data exposure that could include 3,159,770 usernames, emails, names, surnames, addresses, zip codes, cities, phones, and birthdates. The exposure would have happened in January 2025 although it was reported in January 2026.
wired.com	The site wired.com has been reported to possibly have suffered a data exposure that could include 2,366,577 emails, phones, names, surnames, birthdates, usernames, states, zip codes ,addresses, and cities. The possible exposure would have happened in December 2025 although it was reported in January 2026.

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

www.constella.ai

constella/