Constella

Monthly Business Review

April 1st to April 30th, 2026

Date_May 2026

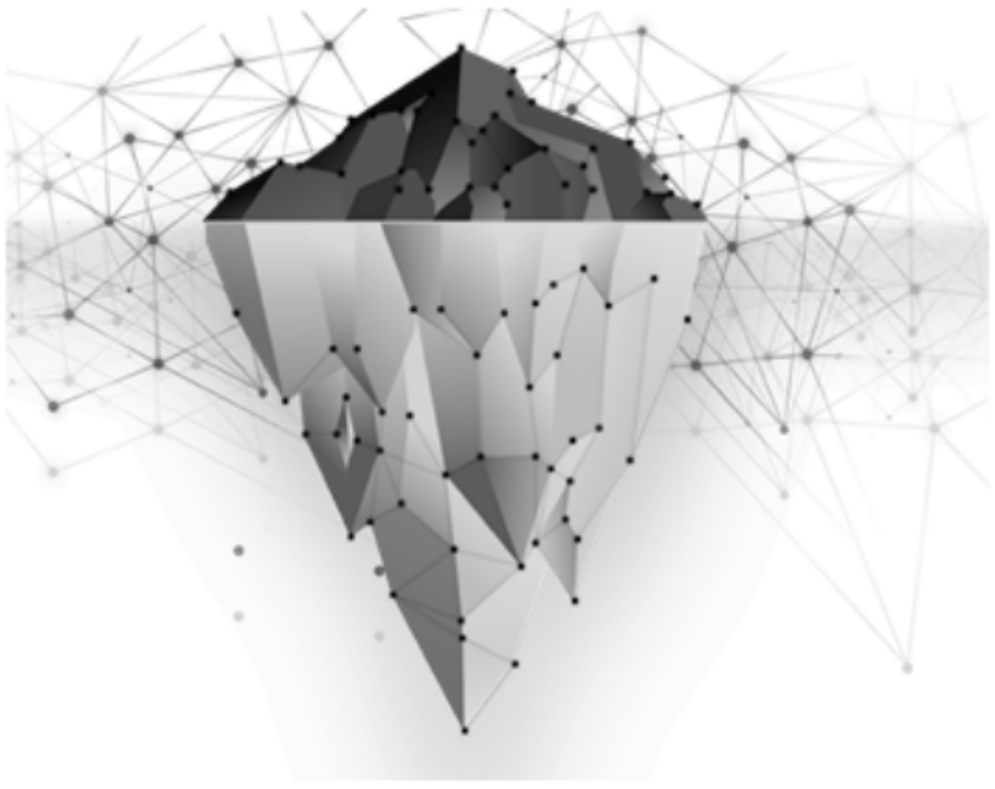
Table of Contents

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	320+ Million	500+ Million	53+
Processed Assets	Alerts Triggered	Assets Monitored	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 **April 1st to April 30th, 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	13,377,097,971

The total number of breaches found in the month:

New Breaches Found

Period	Num
Month	41,352

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

Cleansed Identities

Period	Num
Month	12,863,260,077

**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	7,512,301,833
Leaked / Unknown	5,202,064,845
Combo Breaches	513,837,894
Hacked	148,893,399

Statistics Charts

3.1 Monthly Breaches - Data Distribution (April 2026)

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

1,215,438,662
Email

606,423,349
Password

559,796,363
Name

616,997,138
Username

64,834,711
IP Address

352,157,755
Geographic Location

254,928,275
Birthdate

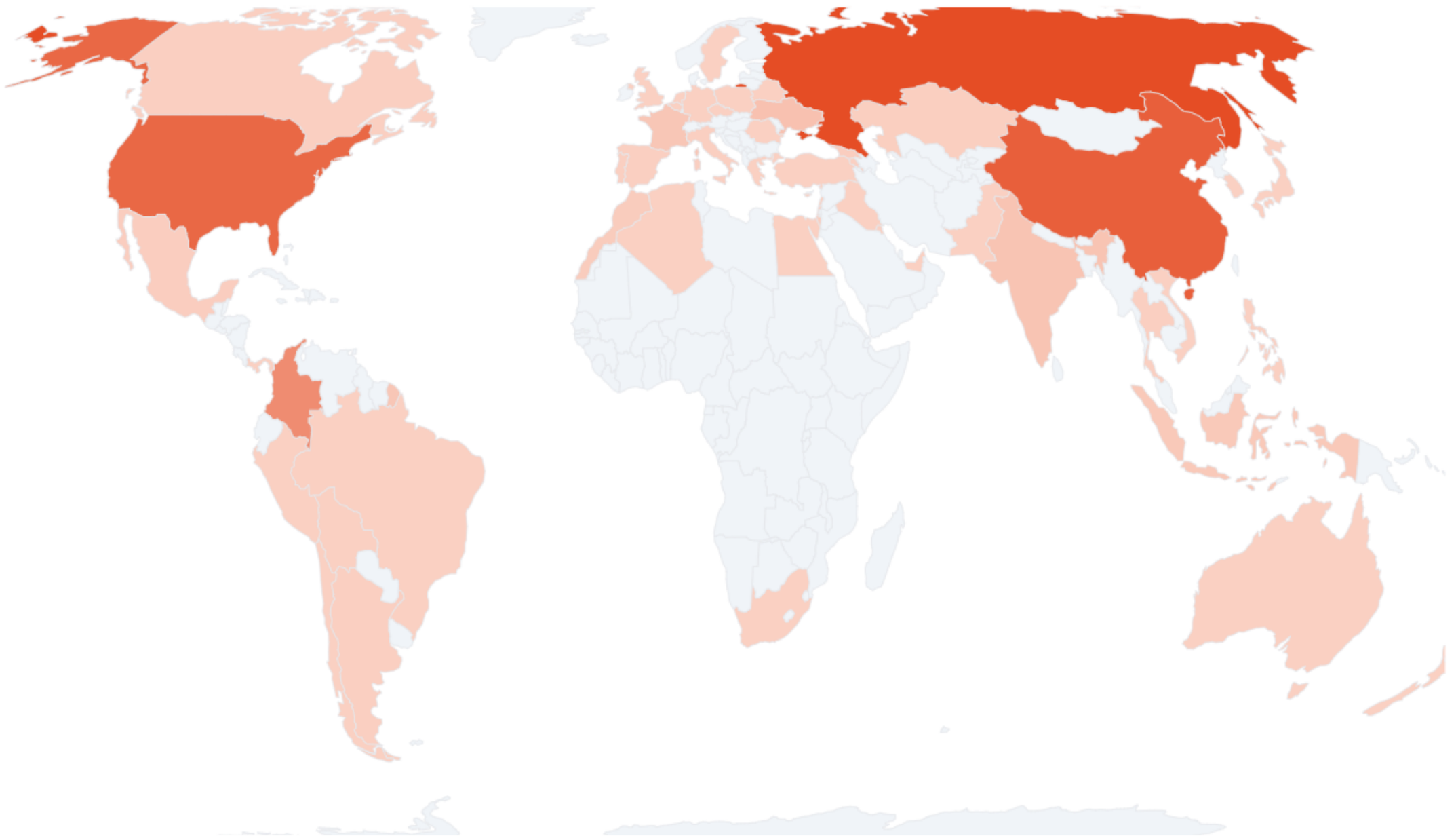
775,449,075
Phone number

501,891
Bank Account

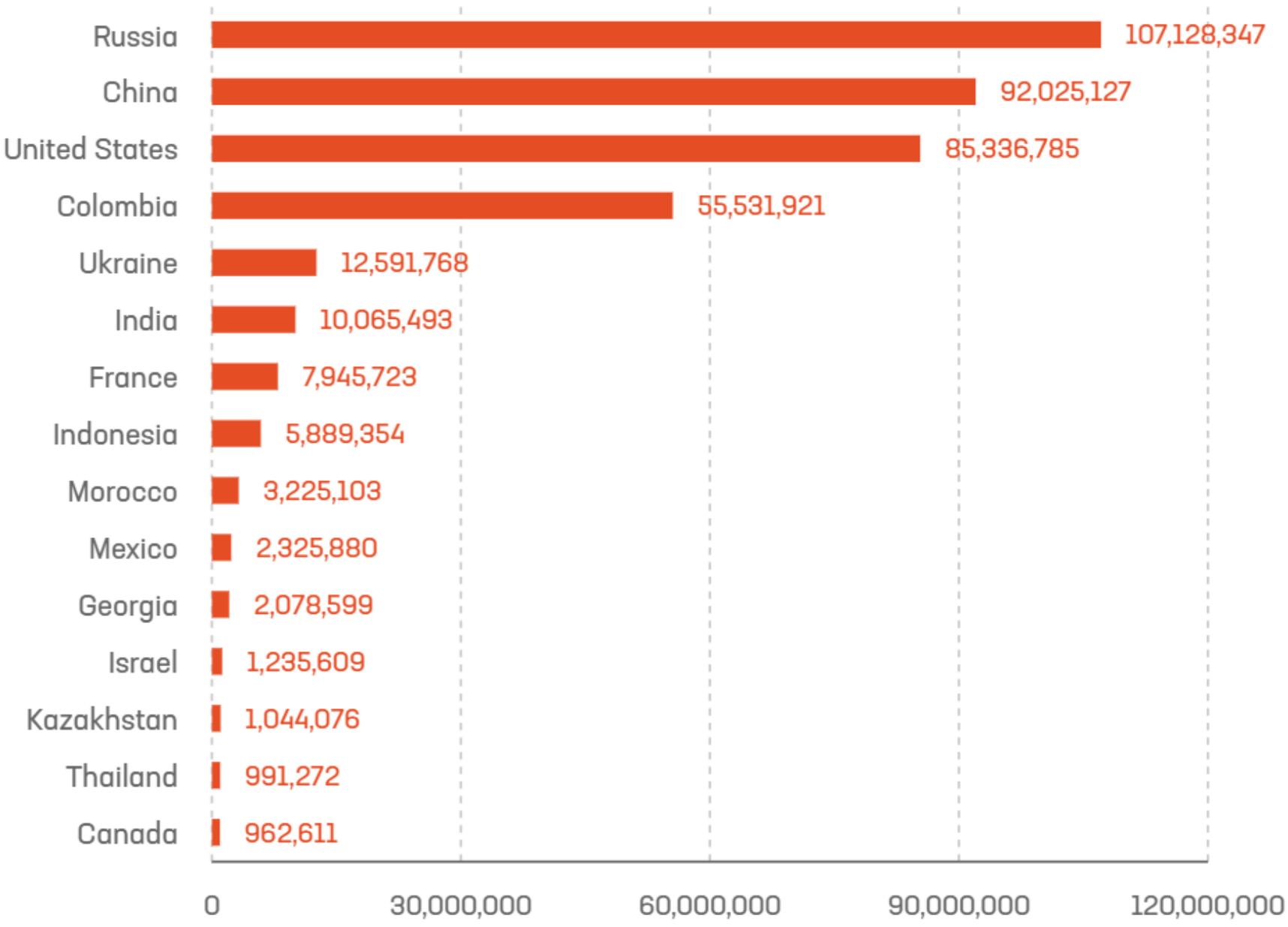
15,622,002
SSN

3.2 Geographic Distribution of Breaches (April 2026)

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

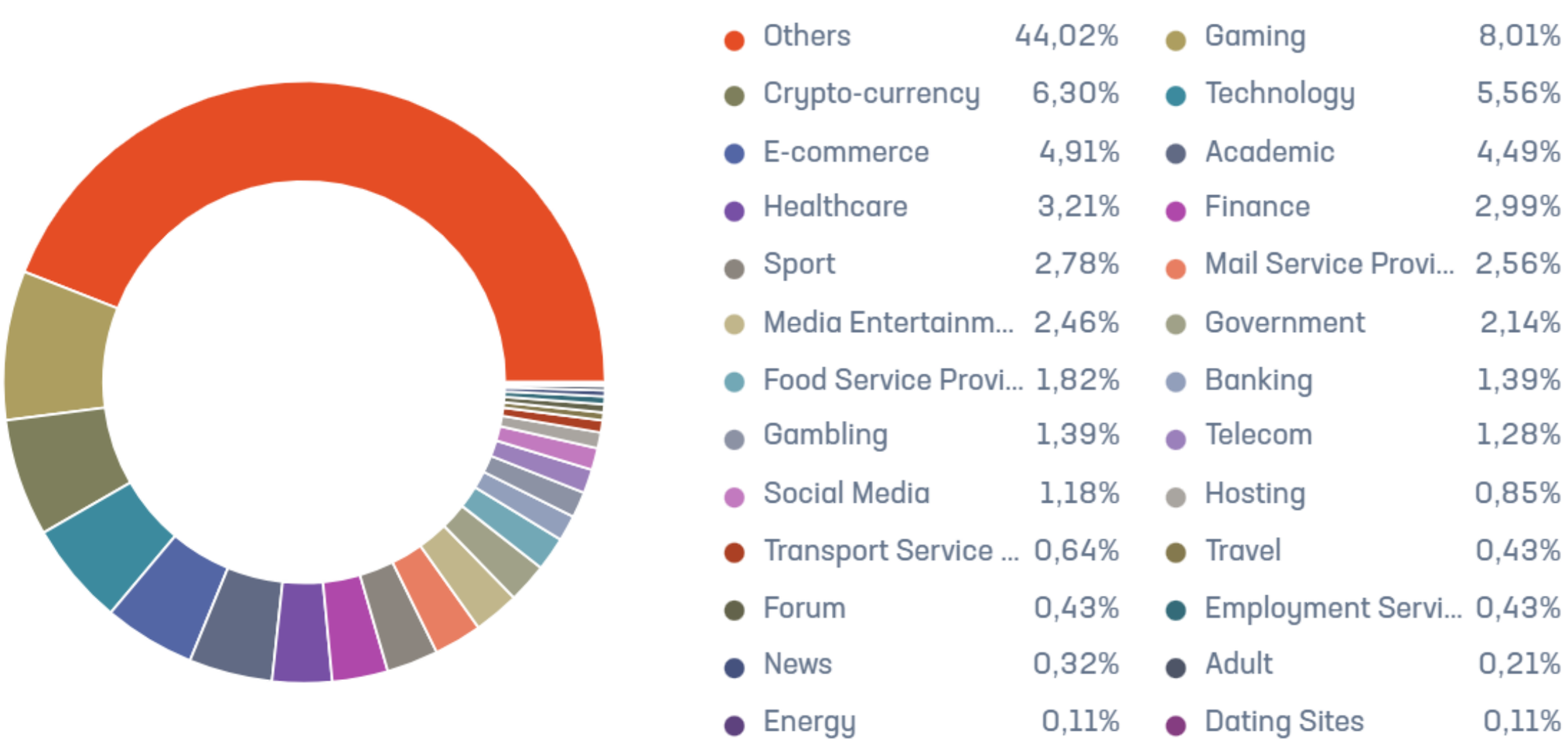


Geographic Location



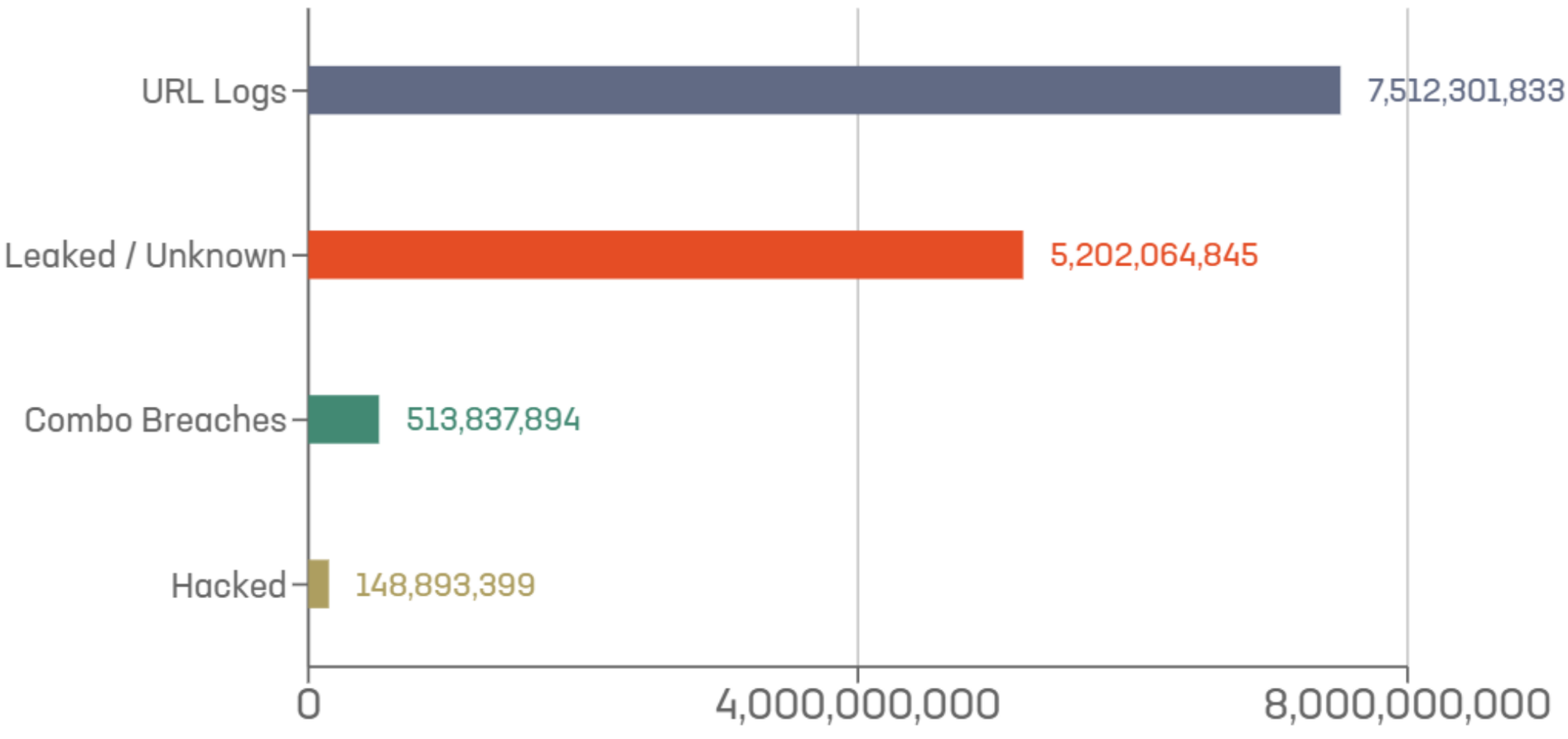
3.3 Distribution of incidents by Category (April 2026)

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



3.4 Number of Identities Exposed by Type (April 2026)

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



3.5 Breach Distribution by Password Encryption Type (April 2026)

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

No Passwords	719 (58.31%)	Plaintext	349 (28.30%)
Blowfish	21 (1.70%)	bcrypt	21 (1.70%)
MD	19 (1.54%)	SHA	17 (1.38%)
SHA	17 (1.38%)	Skein	10 (0.81%)
NTLM	10 (0.81%)	PHPs	7 (0.57%)
Joomla	7 (0.57%)	WordPress	7 (0.57%)
Unknown	7 (0.57%)	HAVAL	6 (0.49%)
Tiger	4 (0.32%)	MySQL	3 (0.24%)
Radmin	3 (0.24%)	DNSSEC	2 (0.16%)
Snefru	2 (0.16%)	GOST	2 (0.16%)

Top Featured Breaches/ Incidents Detected

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

Top Breaches from April 1st to April 30th, 2026

Breach Name	Description
carnivalcorp.com	The site carnivalcorp.com has been reported to have suffered a data exposure that could include 16,332,137 emails, states, names, surnames, birthdates, and phones. The possible exposure was reported in April 2026.
bosco.ru	The site bosco.ru has been reported to possibly have suffered a data exposure that could include 6,896,921 usernames, passwords, names, surnames, emails, birthdates, phones, cities, addresses, and ip addresses. The possible exposure would have happened in March 2026 although it was reported in April 2026.
ecoledirecte.com	The site ecoledirecte.com has been reported to possibly have suffered a data exposure that could include 6,610,344 names, surnames, birthdates, phones, and emails. The possible exposure was reported in April 2026.
jamendo.com	The site jamendo.com has been reported to possibly have suffered a data exposure that could include 6,444,071 emails, and usernames. The possible exposure was reported in April 2026.
hallmark.com	The site hallmark.com has been reported to possibly have suffered a data exposure that could include 2,858,915 emails, states, phones, names, surnames, zip codes, cities, addresses, and birthdates. The possible exposure was reported in April 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

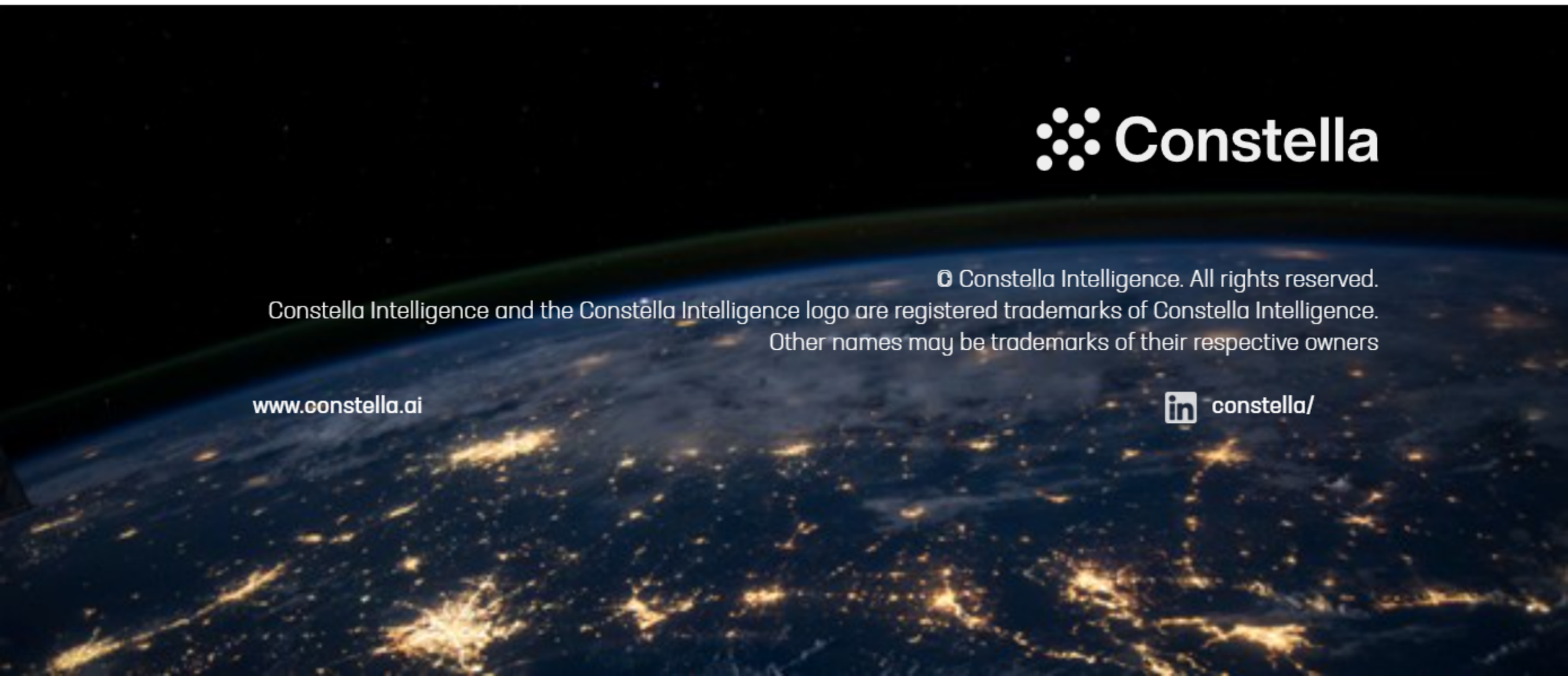
We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web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



www.constella.ai

constella/