

Monthly Business Review

August 1st to August 31st, 2026



Table of Contents

Introduction 3

What is an Incident? 4

What is Accidental Exposure? 4

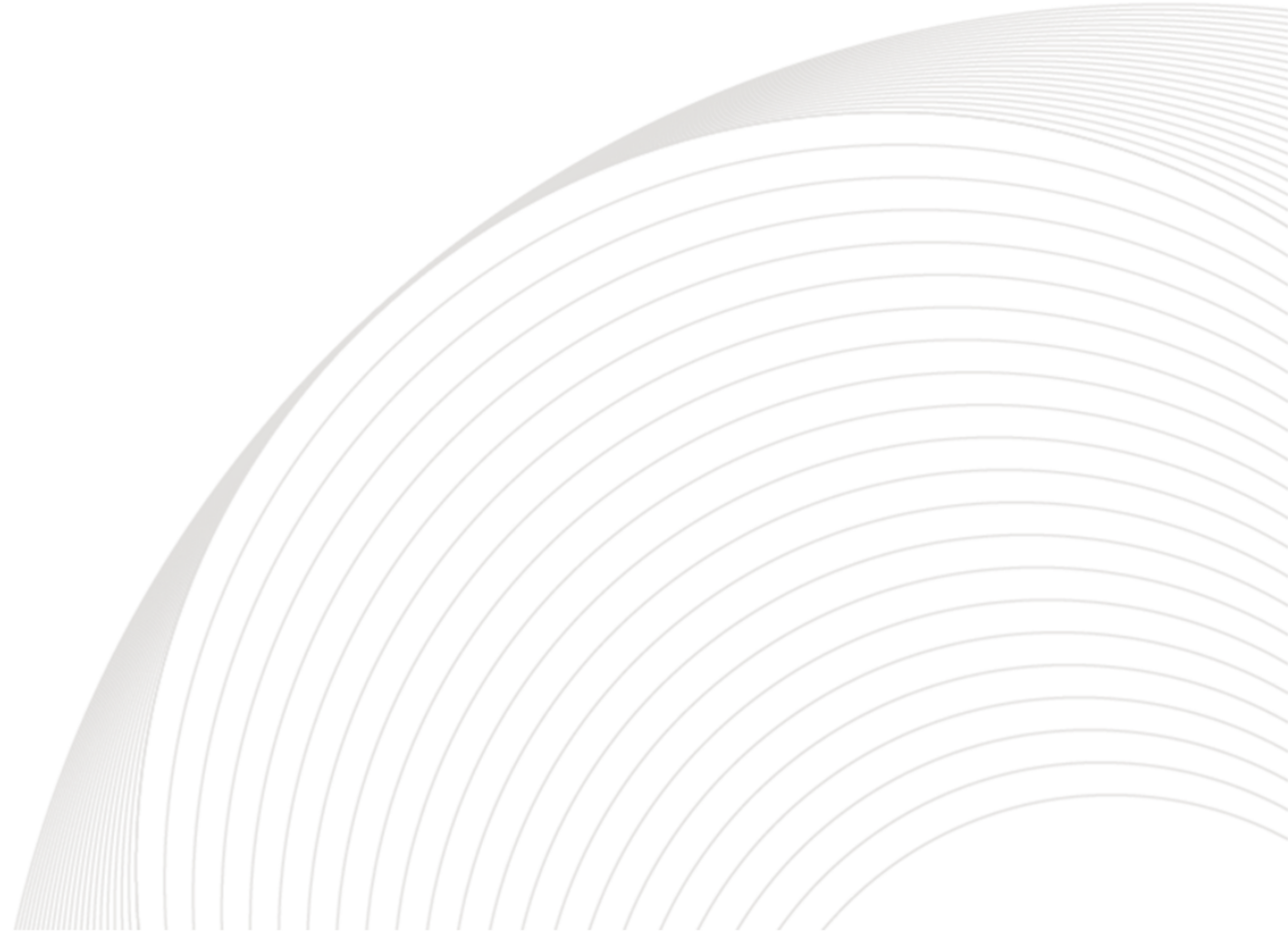
Report Content 5

Statistics Charts 7

Top Featured Breaches/ Incidents Detected 11

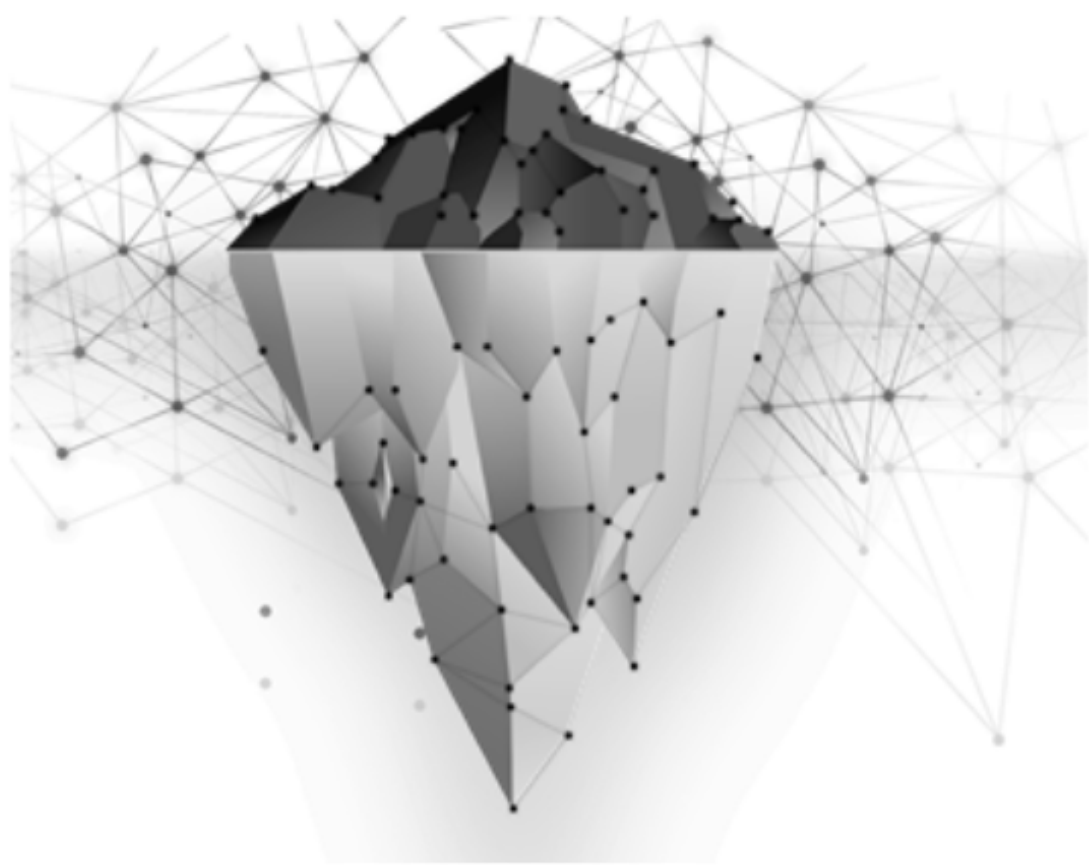
Disclaimer

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.

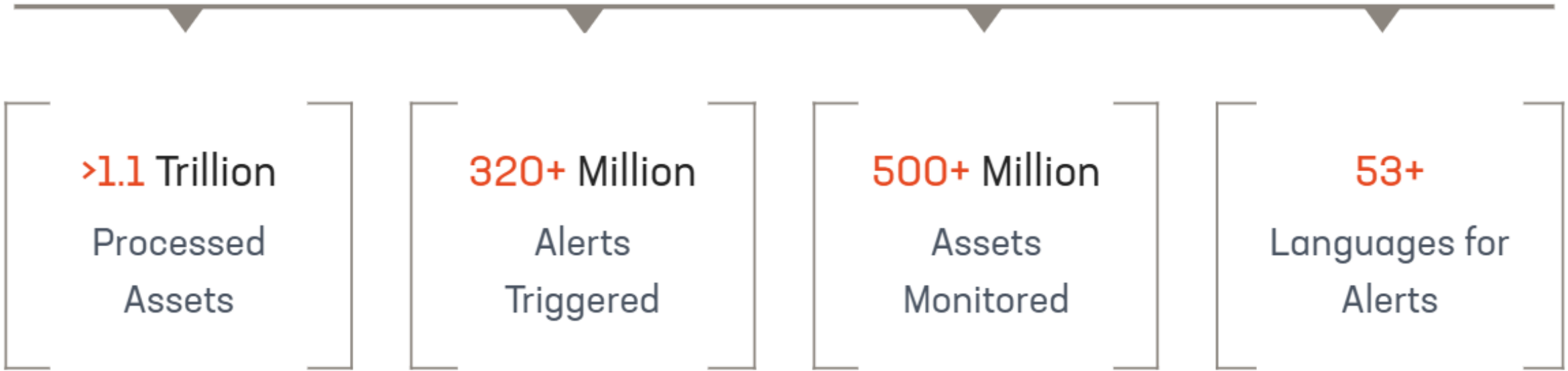


Introduction

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?

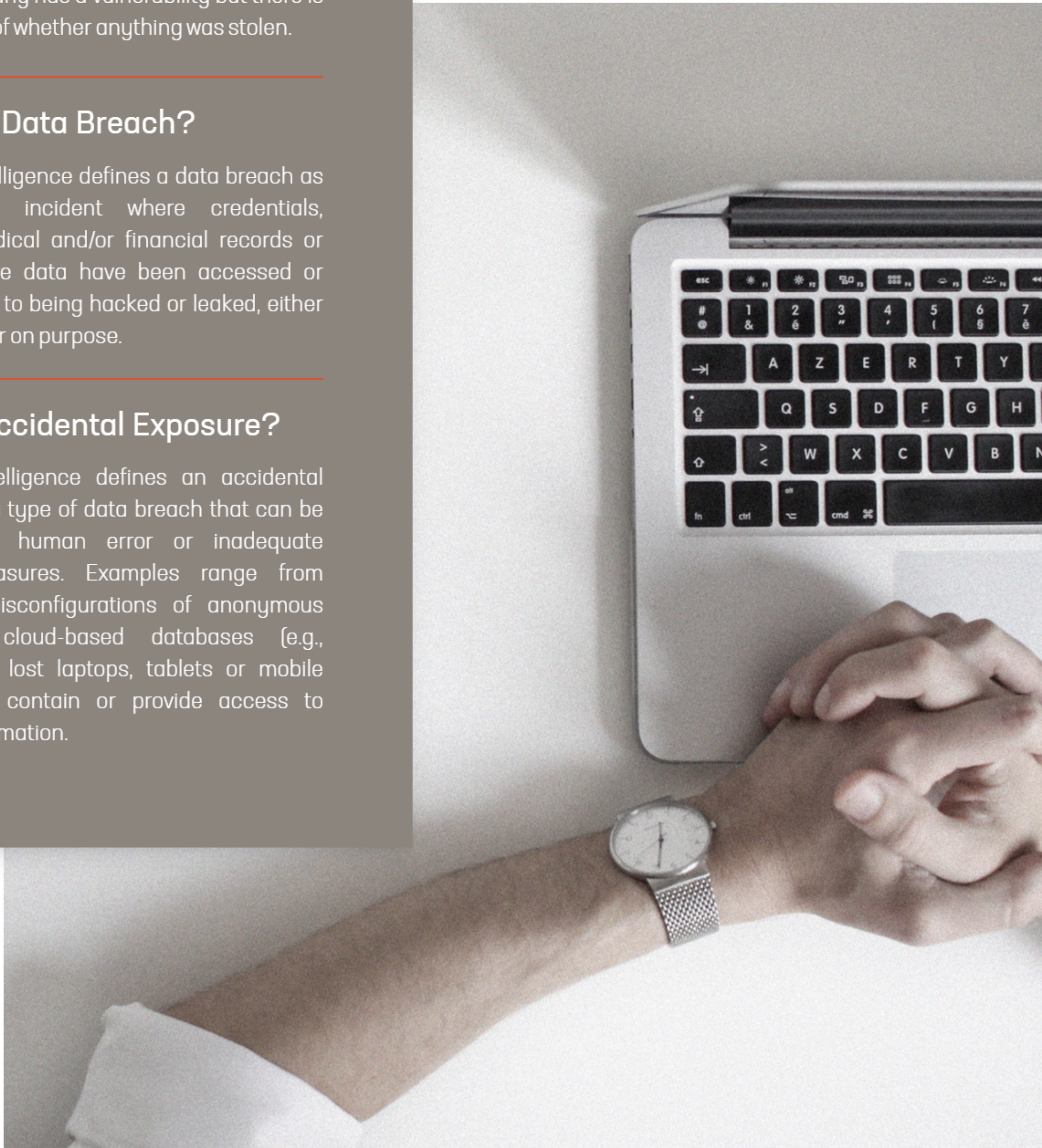
Constella Intelligence defines an incident as when a company has a vulnerability but there is confirmation of whether anything was stolen.

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 **August 1st to August 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	23,366,498,777

The total number of breaches found in the month:

New Breaches Found

Period	Num
Month	79,974

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

Cleansed Identities

Period	Num
Month	17,341,979,345

**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	13,012,997,088
Combo Breaches	6,024,519,432
Leaked / Unknown	4,120,562,585
Hacked	208,419,672

Statistics Charts

3.1 Monthly Breaches - Data Distribution (August 2026)

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



1,790,397,218
Email



1,249,220,426
Name



196,439,431
IP Address



857,164,983
Birthdate



239,107,582
Bank Account



1,178,983,982
Password



1,066,014,483
Username



904,784,467
Geographic Location



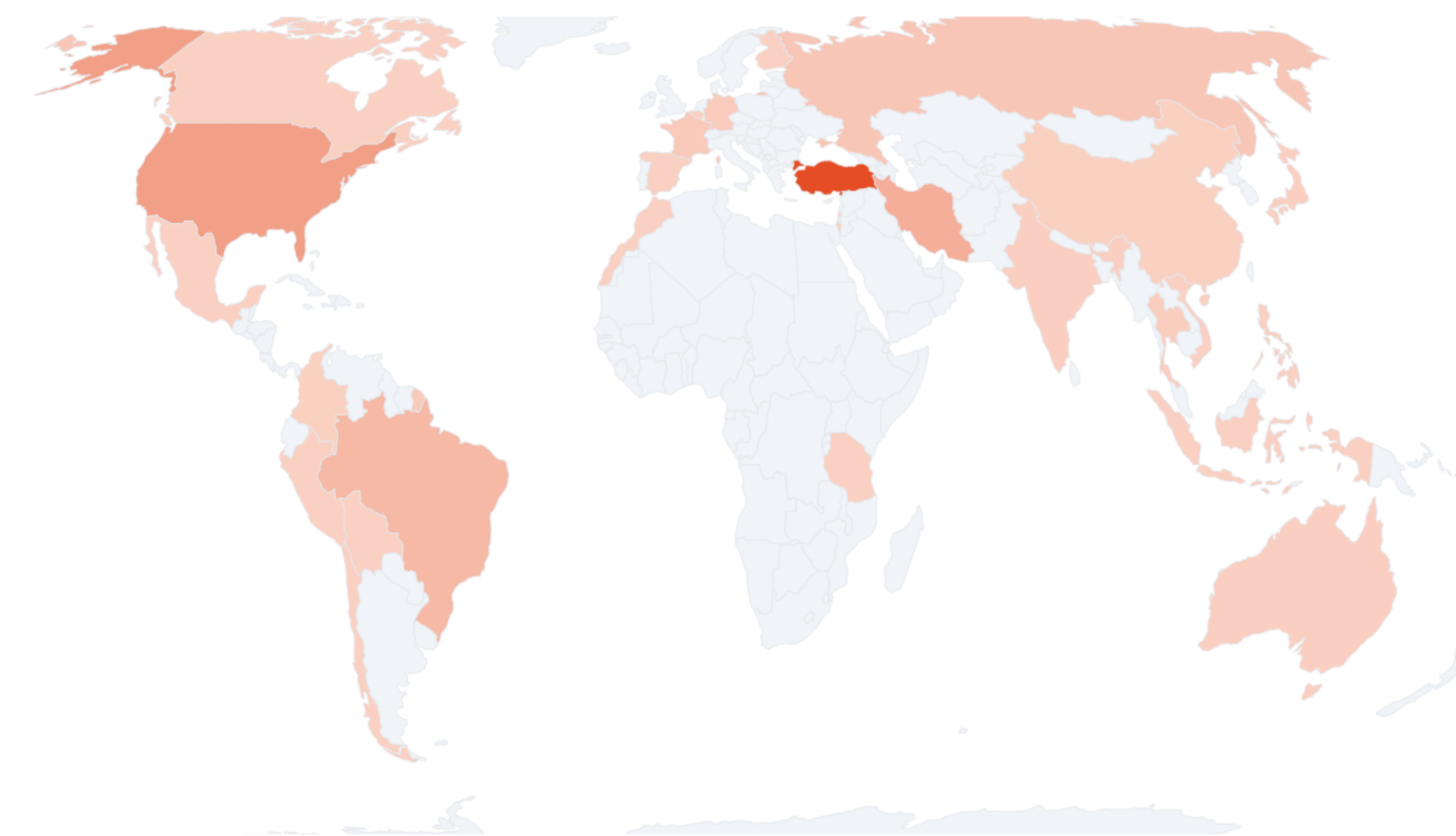
1,251,686,380
Phone number



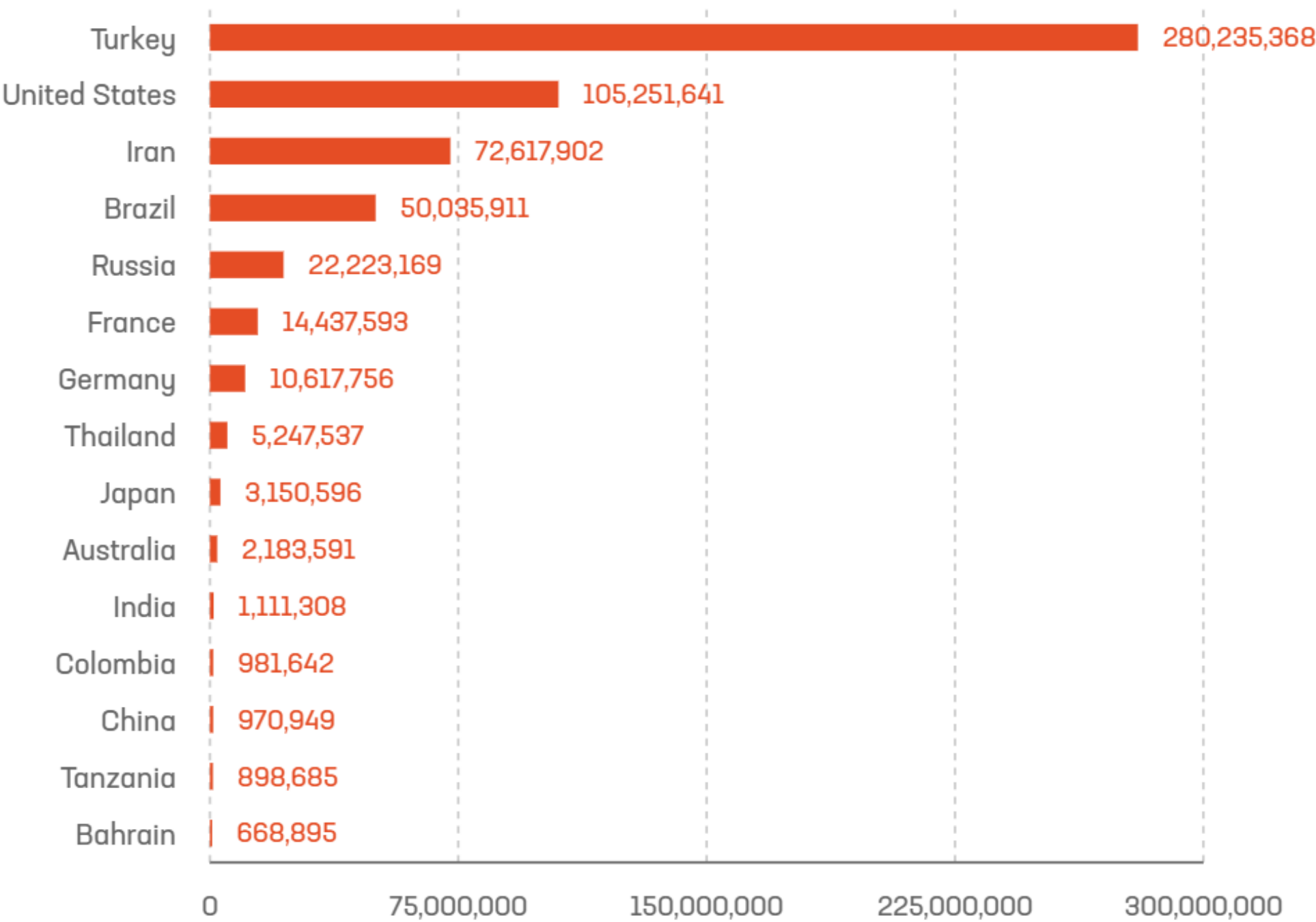
34,133,178
SSN

3.2 Geographic Distribution of Breaches (August 2026)

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

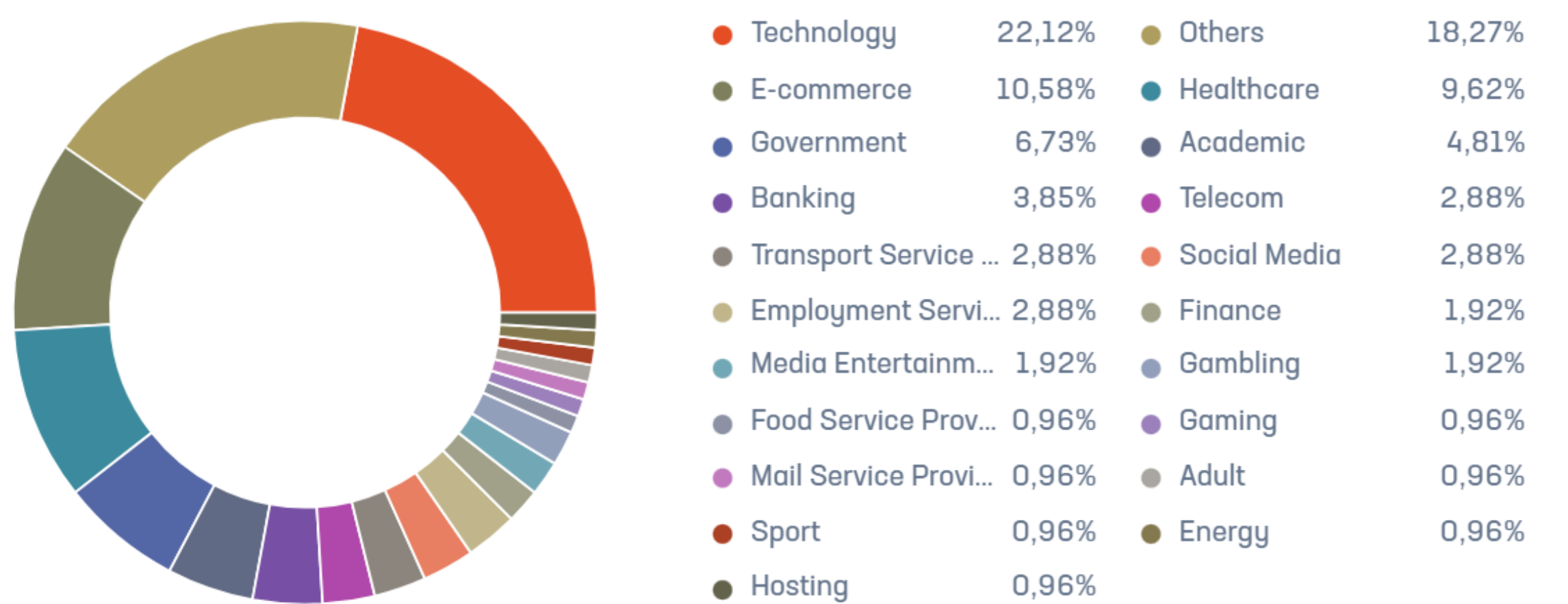


Geographic Location



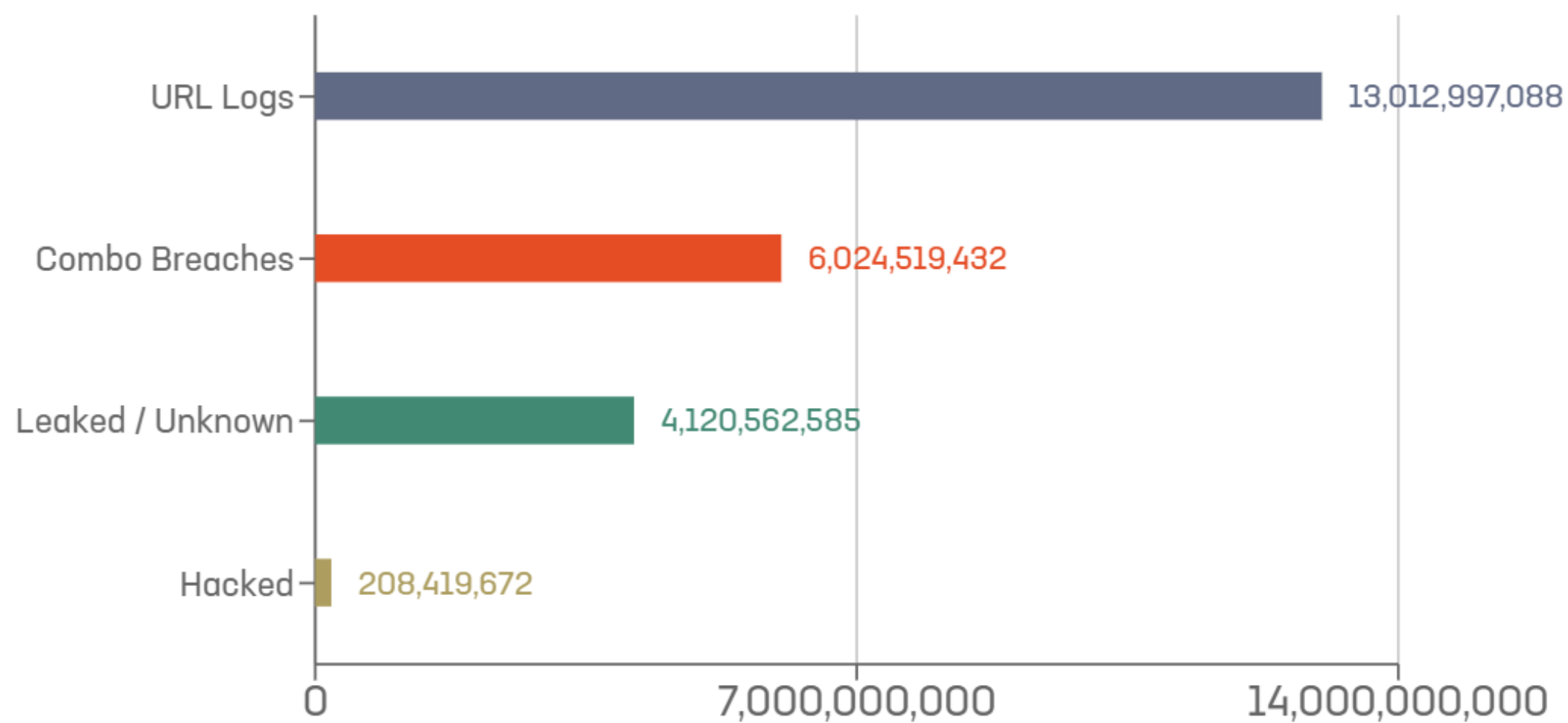
3.3 Distribution of incidents by Category (August 2026)

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



3.4 Number of Identities Exposed by Type (August 2026)

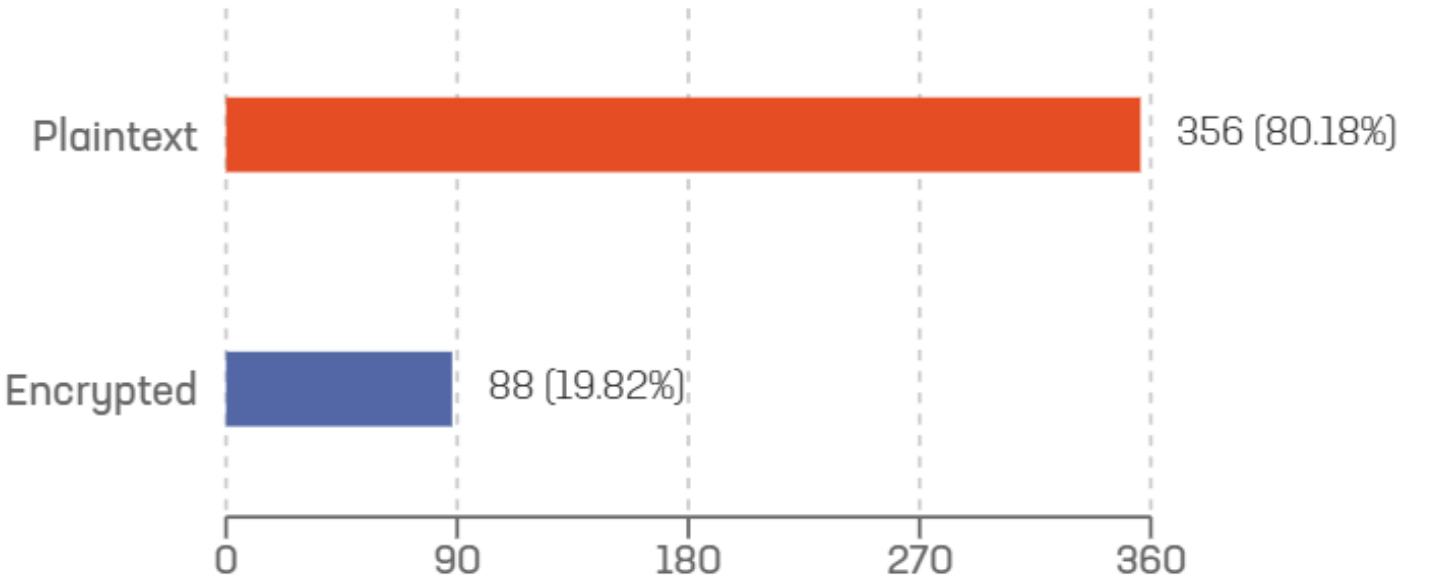
The following chart represents the number of identities detected during August 2026 by its type:



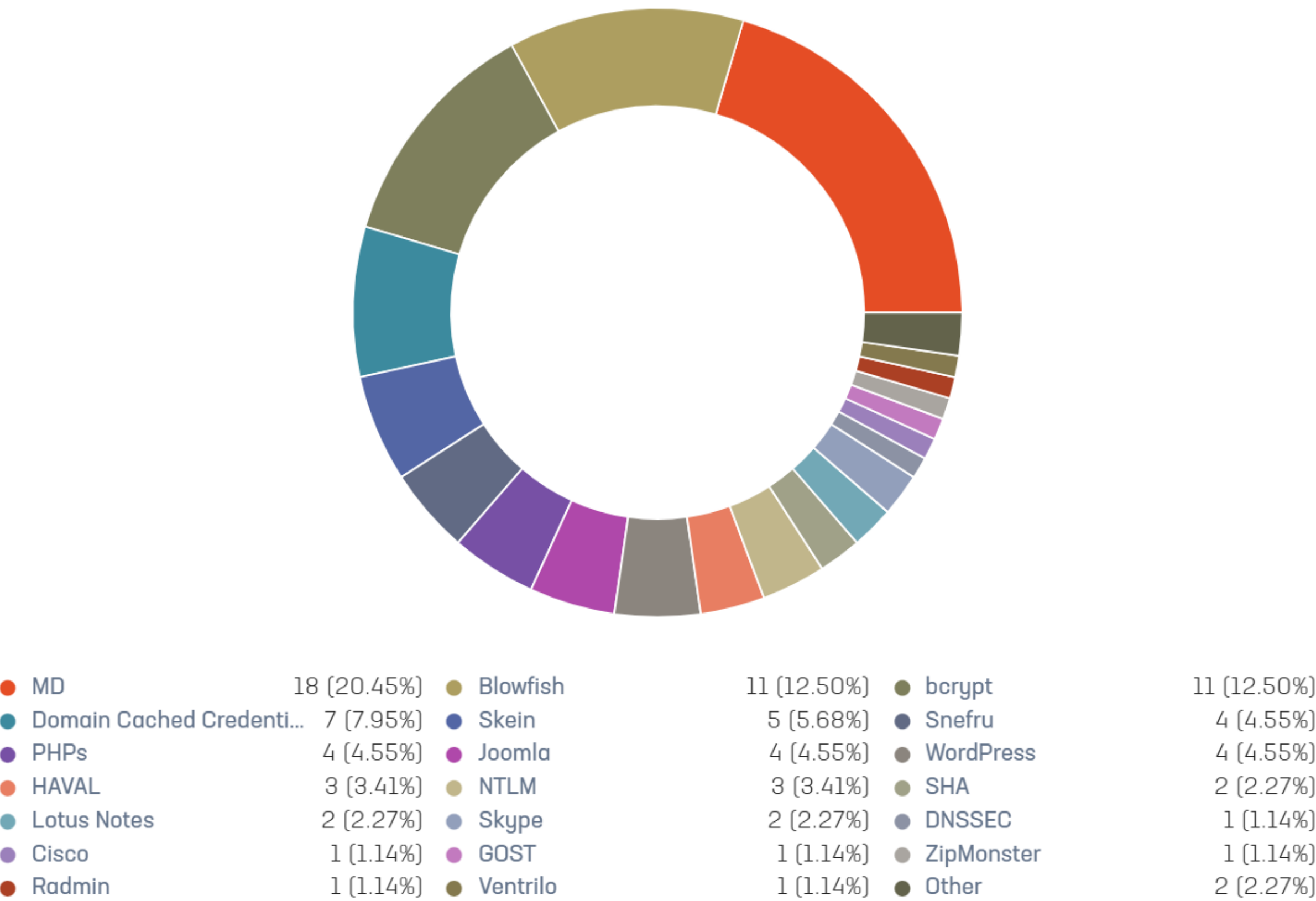
3.5 Breach Distribution by Password Encryption Type (August 2026)

The following charts compare plaintext credentials against encrypted credentials and show the percentage distribution of encryption algorithms reported during **August 2026** coming from analyzed identities:

Plaintext vs Encrypted



Encryption Algorithm Distribution



Top Featured Breaches/ Incidents Detected

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

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

Breach Name	Description
sermilweb.eb.mil.br	The site sermilweb.eb.mil.br has been reported to possibly have suffered a data exposure that could include 47,809,884 addresses, birthdates, cities, emails, names, surnames, phones, and zip codes. The possible exposure was reported in August 2026.
carhartt.com	The site carhartt.com has been reported to possibly have suffered a data exposure that could include 45,598,898 emails, phones, names, surnames, companies, addresses, cities, states, zip codes, usernames, and birthdates. The possible exposure was reported in August 2026.
exactsciences.com	The site exactsciences.com has been reported to possibly have suffered a data exposure that could include 30,518,067 names, surnames, emails, usernames, phones, addresses, cities, states, zip codes, birthdates, and ssn. The possible exposure was reported in August 2026.
ringcentral.com	The site ringcentral.com has been reported to possibly have suffered a data exposure that could include 30,162,786 zip codes, cities, addresses, emails, phones, birthdates, names, surnames, states, and username. The possible exposure was reported in August 2026.
mosgorzdrav.ru	The site mosgorzdrav.ru has been reported to possibly have suffered a data exposure that could include 5,379,520 surnames, names, birthdates, phones, insurance names, and addresses. The possible exposure was reported in August 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 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/)