RESTECH SOLUTIONS

MOHTHLY ILLUMINATIONS

LIGHTING THE DARK WEB℠

fEBRUARY 2020

ResTech Solutions

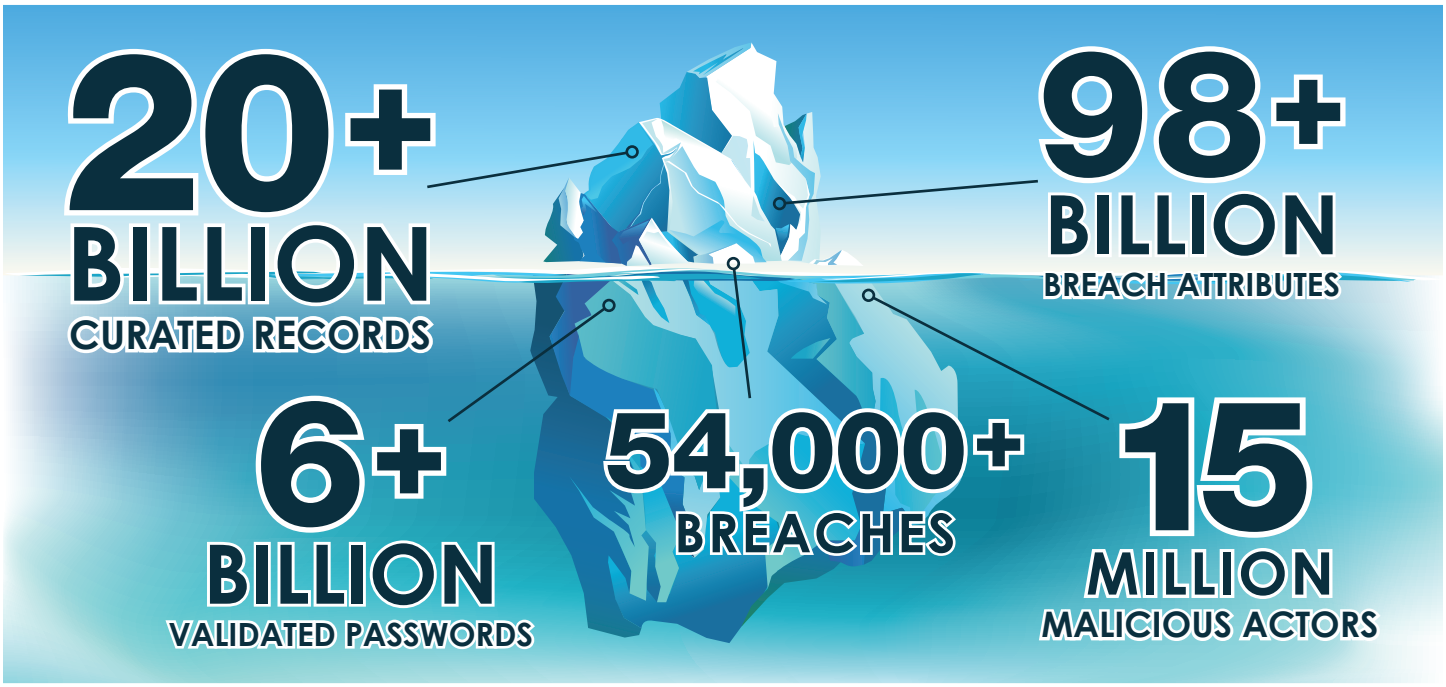
Solutions for a Human World

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. ResTech Solutions 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.

1. 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. ResTech Solutions monitors the surface, social, deep and dark web detecting exposed identities and stolen data helping consumers and companies manage the risk.



WHAT IS AN INCIDENT?

ResTech Solutions defines an incident as when a company has a vulnerability but there is no confirmation of whether anything was stolen.

WHAT IS A DATA BREACH?

ResTech Solutions 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?

ResTech Solutions 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.

2. REPORT CONTENT

All of the data breach information used in this report has been aggregated from the ResTech Solutions database between December 1st to December 31st, 2019. 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	Number
December 2019	**1,797,497,700**

The total number of breaches found in the month:	
NEW BREACHES FOUND	
Period	Number
December 2019	**287**

The total number of exposed identities after cleaning duplicates and fake data:	
CLEANSED IDENTITIES	
Period	Number
December 2019	**675,749,845**
**Note: Due that combo lists 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):	
CLEANSED IDENTITIES	
Type	Number
Unattributed	**27,173,987**
Hacked / Leaked	**648,575,858**
Combo Breaches	**1,121,747,855**

3. STATISTICS CHART

3.1 Monthly Breaches - Data Distribution

(December 2019)

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

648,478,553
EMAIL

18,243,104
PASSWORD

3,585,476
SALT

6,099,510
USERNAME

338,768,838
IP ADDRESS

636,982,978
NAME

3,447,560
BIRTHDATE

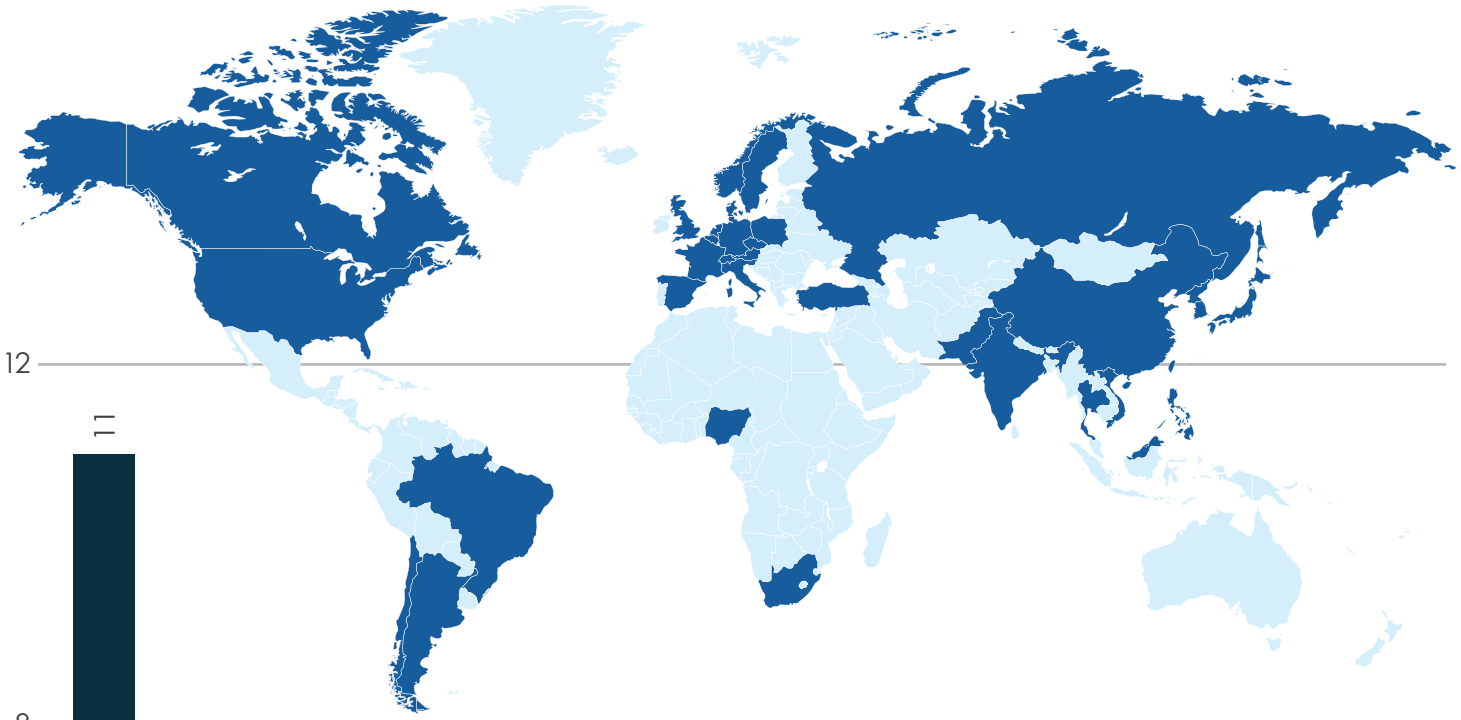
342,290,383
PHONE NUMBER

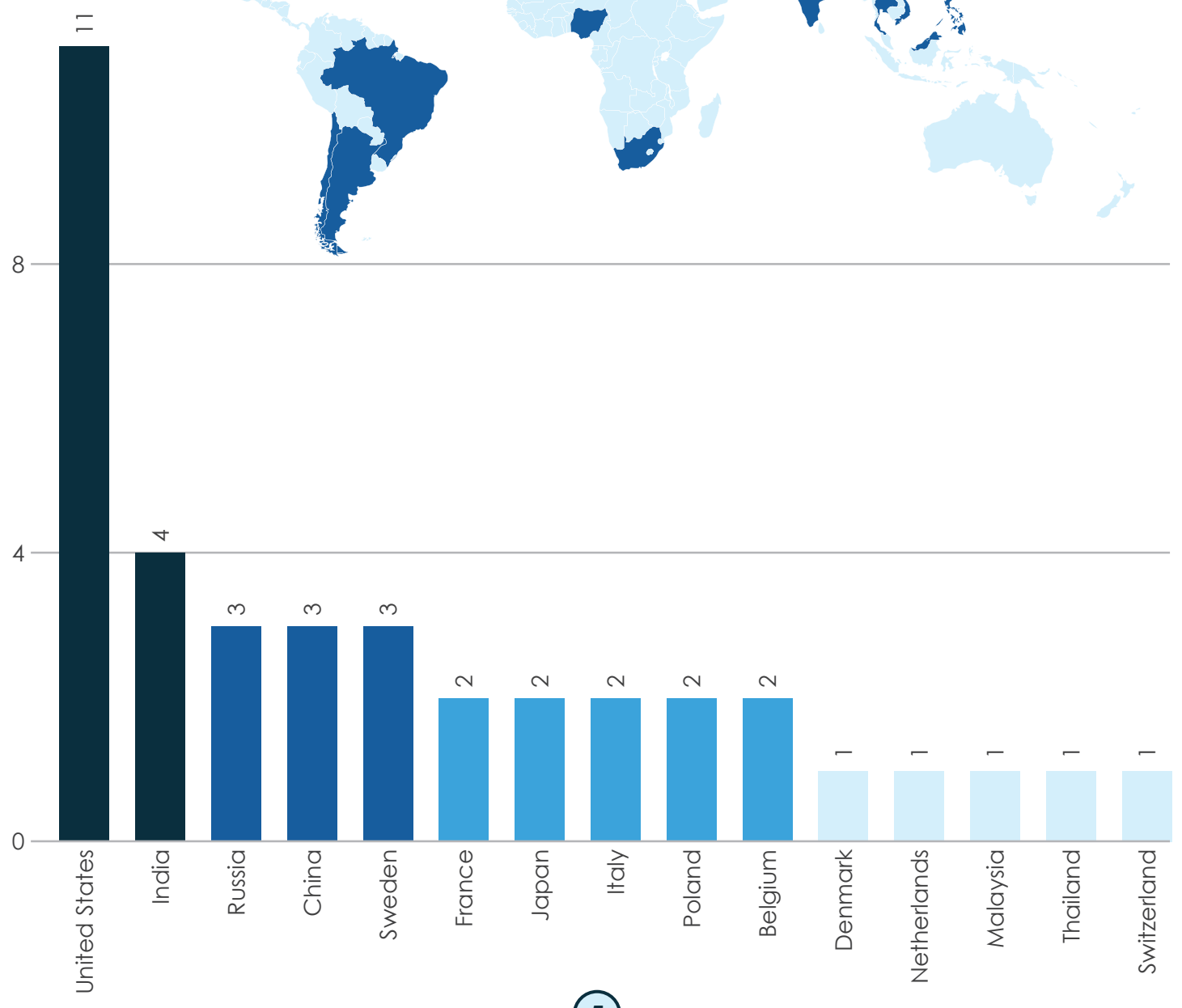
3,447,560
BIRTHDATE

297,147,843
SOCIAL

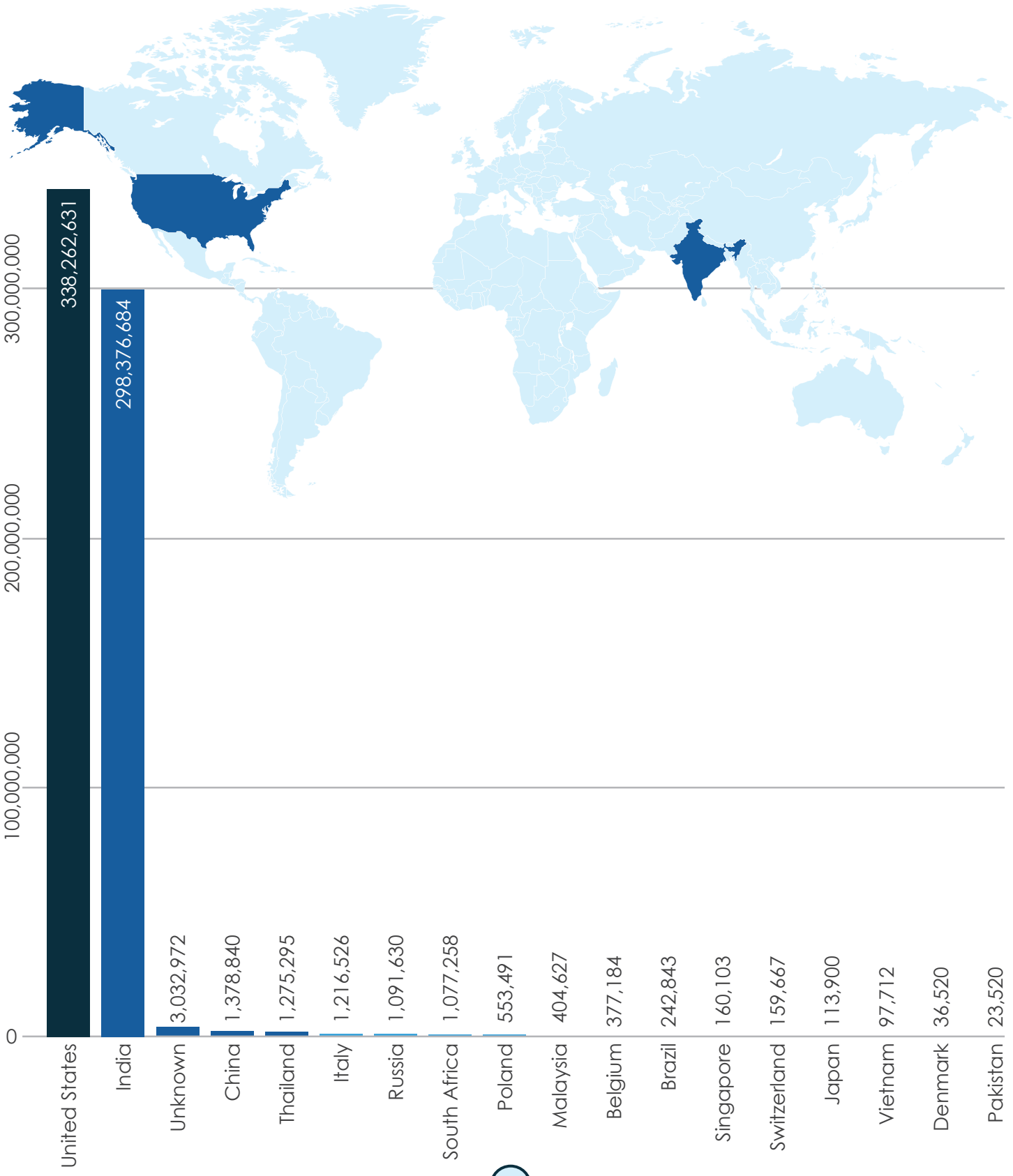
3.2 Geographic Distribution Of Breaches (December 2019)

The following map represents the total number of breaches reported during **December 2019** geographically coming from cleansed identities:



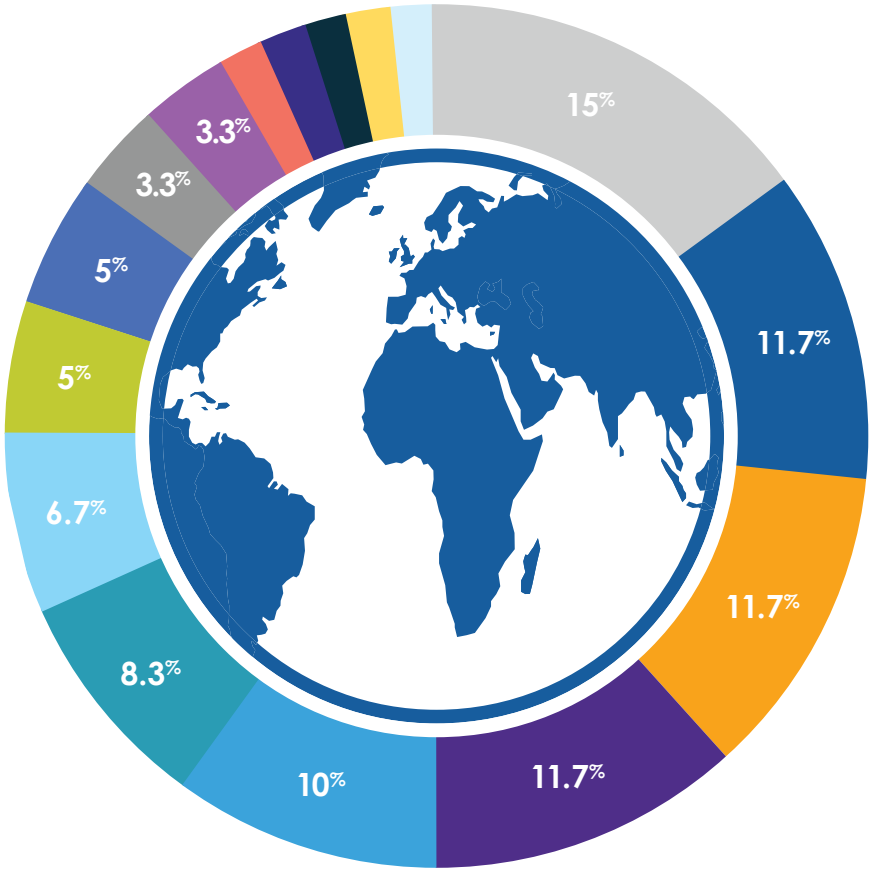


The following map represents the total number of records reported during **December 2019** geographically coming from cleansed identities:



3.3 DISTRIBUTION OF INCIDENTS BY CATEGORY (December 2019)

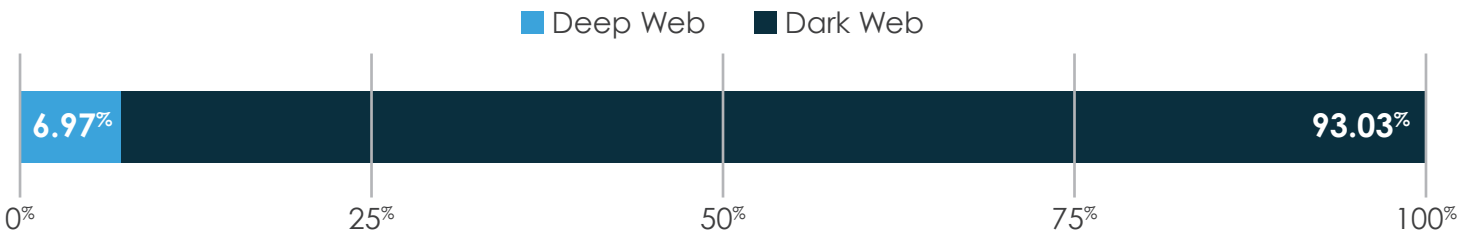
The following chart represents the percentage of breaches reported during **December 2019** by its category coming from cleansed identities:



- Media 15%
- Gaming 11.7%
- Others 11.7%
- Academic 11.7%
- E-Commerce 10%
- Bitcoin 8.3%
- Forum 6.7%
- Technology 5%
- Service Providers 5%
- Business 3.3%
- Health 3.3%
- Adult 1.7%
- Transport 1.7%
- Gambling 1.7%
- Hacking Forum 1.7%
- Social Media 1.7%

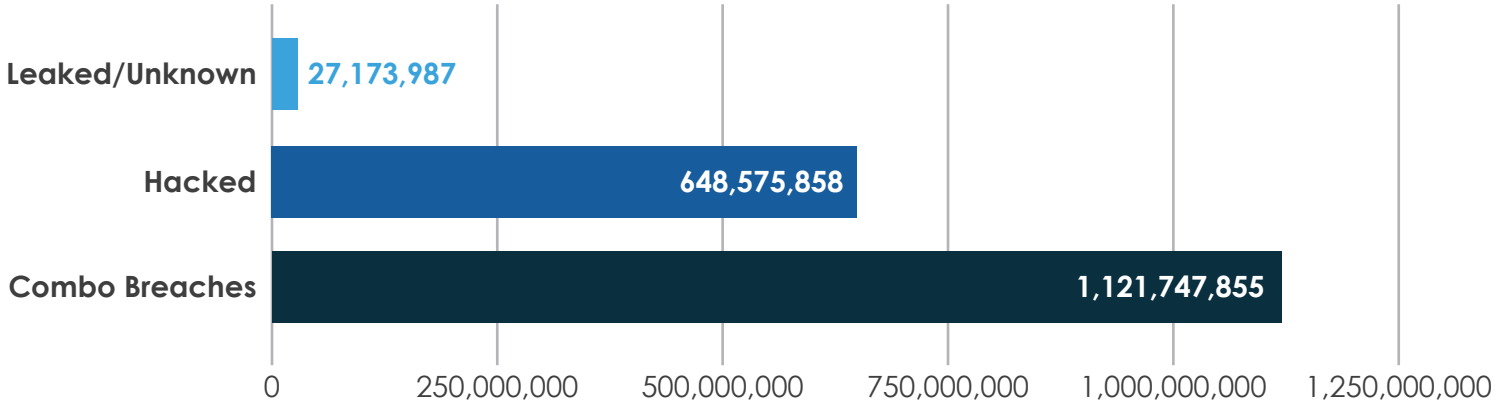
3.4 DISTRIBUTION OF INCIDENTS BY SOURCE OF THE INFORMATION (December 2019)

The following chart represents the percentage of breaches reported during **December 2019** by its source:



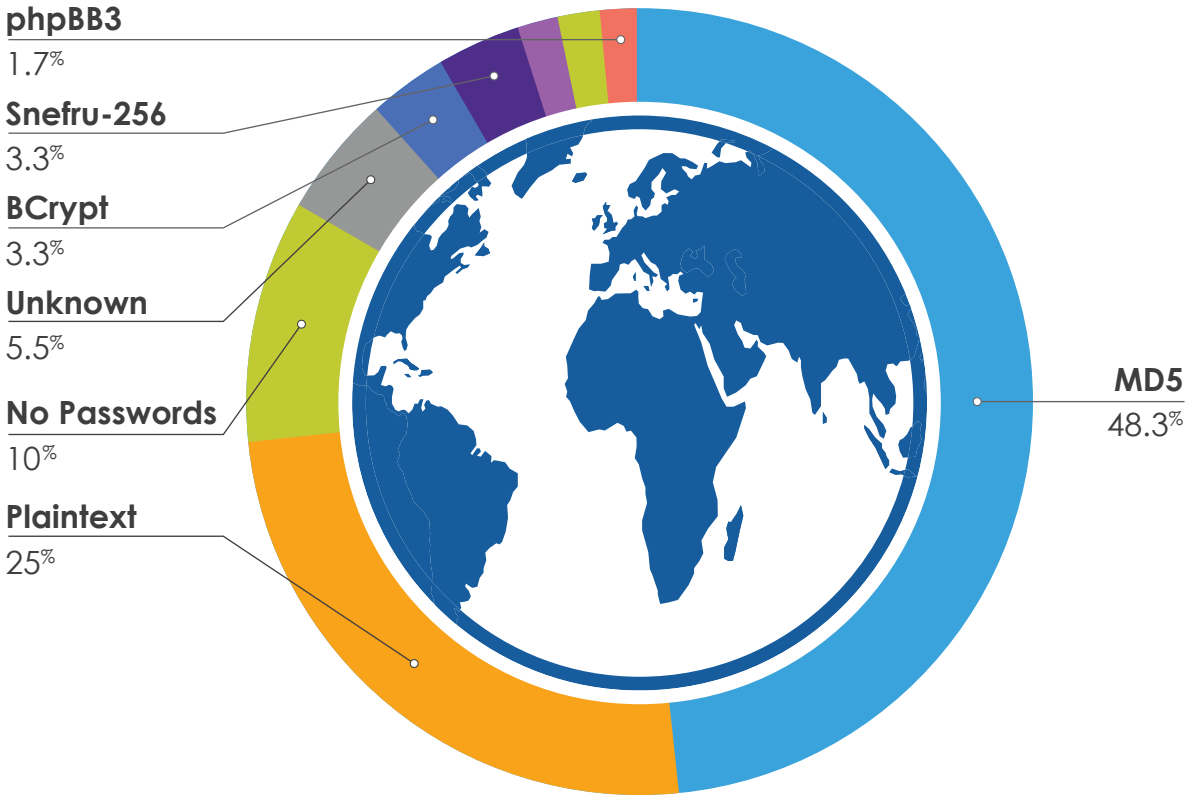
3.5 NUMBER OF IDENTITIES EXPOSED BY TYPE (December 2019)

The following chart represents the number of identities detected during **December 2019** by its type:



3.6 DISTRIBUTION OF INCIDENTS BY PASSWORD ENCRYPTION TYPE (December 2019)

The following chart represents the percentage of breaches reported during **December 2019** by its type of encryption coming from cleansed identities:



4. TOP FEATURED BREACHES/ INCIDENTS DETECTED

The top incidents reported in the month of December 2019 are:

TOP BREACHES FROM DECEMBER 1ST TO DECEMBER 31ST, 2019	
BREACH NAME	**DESCRIPTION**
exactis.com	The site exactis.com has been reported to possibly have suffered a data exposure that could include 335,399,704 emails, names, surnames, phones, zip codes, cities, states, addresses, and IP addresses. The possible exposure would have happened in July 2018 although it was reported in December 2019.
truecaller.com	The site truecaller.com has been reported to possibly have suffered a data exposure that could include 291,620,615 emails, names, surnames, and addresses. The possible exposure would have happened in October 2019 although it was reported in December 2019.
vedantu.com	The site vedantu.com has been reported to possibly have suffered a data exposure that could include 5,193,903 emails, passwords, names, surnames, phones, cities, states, and addresses. The possible exposure would have happened in June 2019 although it was reported in December 2019.
wunjun.com	The site wunjun.com has been reported to possibly have suffered a data exposure that could include 1,275,295 usernames, emails, passwords, names, surnames, birthdates, IP addresses. The possible exposure would have happened in July 2017 although it was reported in December 2019.
onlinebloodbank.com	The site onlinebloodbank.com has been reported in December 2019 to possibly have suffered a data exposure that could include 1,128,031 emails, phones, cities, addresses, birthdates, and medical information.
globalyouthleadersforum.org	The site globalyouthleadersforum.org has been reported to possibly have suffered a data exposure that could include 1,077,258 emails and passwords. The possible exposure would have happened in May 2019 although it was reported in December 2019.

ABOUT RESTECH SOLUTIONS

ResTech Solutions protects identities and companies by scanning the surface, social and deep and dark web for stolen, leaked or lost login credentials and other information.

ResTech Solutions helps organizations measure, monitor and manage digital risk by identifying network users with stolen credentials, the single greats source of cybercrime on the dark web.

ResTech Solutions notifies organizations and individuals in real time when credentials first appear to guard against the theft of identities, information and money before it happens. We are strong advocates of effective password security protocols as outlined by the National Institute of Standards and Technology (NIST) and embrace their Cybersecurity Framework throughout our company, and in the execution of our services.

RESTECH SOLUTIONS

ILLUMINATING THE DARK WEB[SM]

ResTech Solutions Headquarters
8715 Meadowcroft Dr. #102
Houston, TX 770063

www.restech.solutions