BREACHED DATA ANALYSIS

ALL RIGHTS RESERVED

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

TABLE OF CONTENTS

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

INTRODUCTION TO DATA BREACH

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

INTRODUCTION TO DATA BREACH

In Today's modern era where information is being sold for some amount of money which is critical for the one who is purchasing it. Information can be in any form or format which may be paperless or soundless. To protect critical information the need of information security was established.

Organizations spend a lot in securing their trade secret information from being published or exposed to the competitors or outside the network, but even after doing a lot of investment their information breaches (By staff, By systems, any Weakness of process or procedure) which could lead towards data breaches.

What is Data Breach?

"Breach Data" is data that is made publicly available by individuals or entities that perpetrate data breaches. While the act of the breach itself is illegal, obtaining and using the data after it has been leaked is both lawful and very useful in OSINT investigations. Most of the company breaches are simply usernames/email addresses and passwords, likely obtained from unsophisticated hacking crews scanning the Internet for unprotected servers left open for external connections.

Sensitive data sets are typically executed by more sophisticated actors and are often hacked government sites or protected data servers; Hacked data sets are routinely uploaded and provided (some free and others paid) to the public on various paste or file storage sites and also to more limited audiences via dark web forums or marketplaces.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

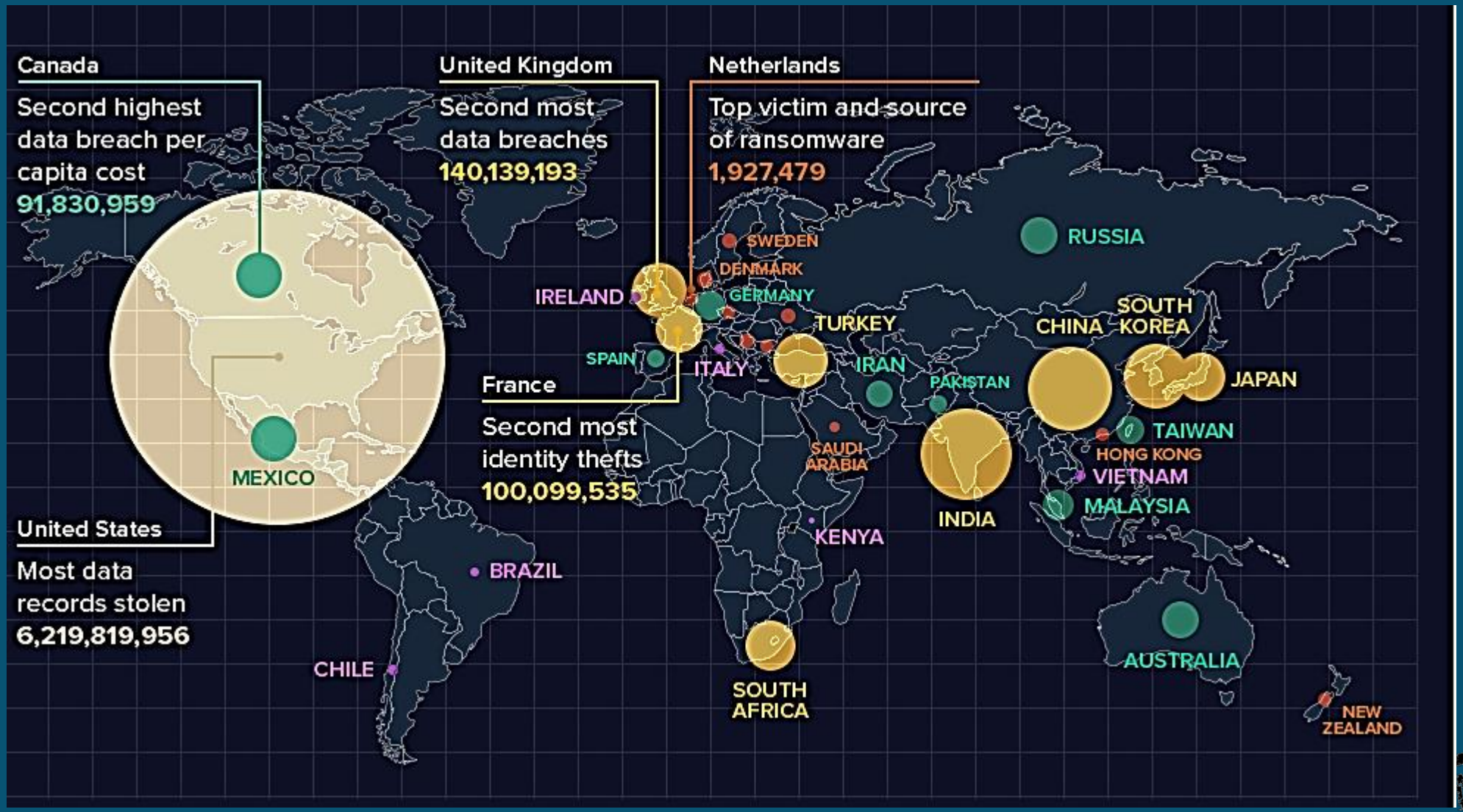
DATA BREACH RECORDS

ALL RIGHTS RESERVED

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

DATA BREACH RECORDS

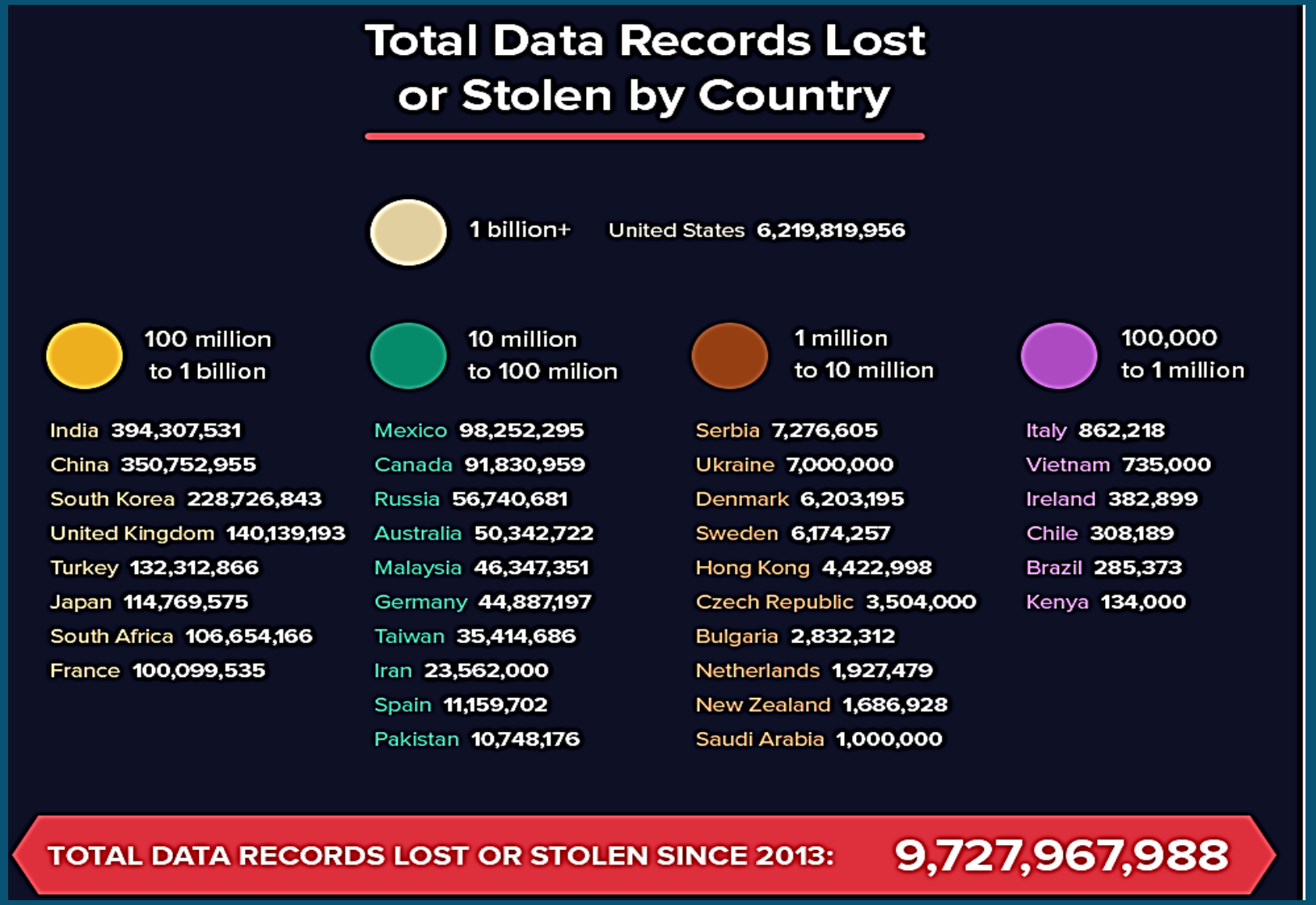
Distribution of breached data records across the world since 2013.



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

DATA BREACH RECORDS



Reference: https://www.varonis.com/blog/wp-content/uploads/2018/07/world-in-data-breaches.png

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

BREACH DATA SOURCES & REFERENCES

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

BREACH DATA SOURCES & REFERENCES

Following are the list of Websites which keeps you update regarding the data breach if happen, it might be conducted using your email address, a company name, username or IP Address.

S.No	Website/ Domain Name	Description	Detect Breach of
1	https://haveibeenpwned.com/	Have I been pwned? is a site to check if you have an account that has been compromised in a data breach. The site came about after what was, at the time, the largest ever single breach of customer accounts	Email Address
2	https://monitor.firefox.com/	get a full report on your compromised accounts and notifications any time your accounts appear in new data breaches.	Email Address
3	https://www.dehashed.com/	DeHashed is a hacked-database search-engine created for security analysts, journalists, security companies, and everyday people to help secure accounts and provide insight on database breaches and account leaks.	Email, IP Address, Username, Phone Number, Domain Name
4	https://ghostproject.fr/	GhostProject.fr is a Fastest Free Database Lookup of Recent 1.4 billion password breach compilation, Ghost Project allows you to Search by email or username.	Email Address, Domain Address
5	https://www.hotsheet.com/inoitsu/	Use this free service to see if an email address is in any hacked data from known breaches	Email Address
6	https://breachdirectory.tk/	BreachDirectory.tk allows you to search through all public data breaches to make sure your emails, usernames, passwords, and domains haven't been compromised.	Email Address, Username
7	https://breachdirectory.com/home?lang=en	BreachDirectory.com allows you to search through all public data breaches to make sure your emails, usernames, passwords, and domains haven't been compromised.	Email Address, Domain Name, IP Address, Username
8	https://vigilante.pw/	Vigilante.pw aims to raise awareness regarding database breaches by providing as much necessary information as possible regarding security breaches.	Domain Name
9	https://sec.hpi.de/ilc/	With the HPI Identity Leak Checker, it is possible to check whether your email address, along with other personal data (e.g. telephone number, date of birth or address), has been made public on the Internet where it can be misused for malicious purposes.	Email Address, Domain Name, IP Address, Username
10	https://emailrep.io/	EmailRep uses hundreds of factors like domain age, traffic rankings, presence on social media sites, professional networking sites, personal connections, public records, deliverability, data breaches, dark web credential leaks, phishing emails, threat actor emails, and more to answer	Email Address

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

BREACH DATA SOURCES & REFERENCES

Following are the list of Websites which keeps you update regarding the data breach if happen, it might be conducted using your email address, a company name, username or IP Address.

S.No	Website/ Domain Name	Description	Detect Breach of
11	https://hunter.io/search/	The Domain Search lists all the people working in a company with their name and email address found on the web. With 100+ million email addresses indexed, effective search filters and scoring, it's Hunter's most powerful email-finding tool.	Email Address
12	https://weleakinfo.com/search?type=email&query=masterubaid@yahoo.com	Get access to an ever growing collection of over 7,000 data breaches. Hundreds of exclusive databases only available on We Leak Info such as Shein, Sephora, and Adult Friend Finder!	Email Address, IP Address, Domain Name, user name
13	https://scylla.sh/	scylla.sh has two major goals. One is to have a community-oriented database leak community that is a useful tool for security researchers.	Email Address
14	https://leak-lookup.com/databases	Leak-Lookup allows you to search across thousands of data breaches to stay on top of credentials that may have been compromised, allowing you to proactively stay on top of the latest data leaks with ease.	Domain Name

ALL RIGHTS RESERVED

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

BREACH DATA FORUMS

ALL RIGHTS RESERVED

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

BREACH DATA FORUMS

In order to monitor data breach, list of forums where information is uploaded at earliest of the breach data. The list is not extensive and doesn't contains the limited links it may vary from forum to forum. But most likely these are the common forums where breach data information is uploaded.

S.No	Website/ Domain Name	Description
1	https://www.reddit.com/r/pwned/ https://twitter.com/haveibeenpwned	These are two of the most active threads posting information about new breach leaks.
2	https://raidforums.com/Announcement-Database-Index-CLICK-ME	This forum contains thousands of dataset of compromised websites which is being sold for thousands of dollar
3	https://nuclearleaks.com/	This site has a great list of historical breaches, the original date of breach, number of records compromised, and hashing algorithm (very helpful to know whether you are getting a .txt file or a list of hashed passwords, for example). This site does not allow for downloads of the breach files themselves and instead claims its primary purpose is to raise awareness about database breaches.
4	https://databases.today/	This site claims it has "the biggest free-to-download collection of publicly available website databases for security researchers and journalists." The site contains 1385 databases (totalling 73 gigabytes) of the most popular leaks over recent years (LinkedIn, Ashley Madison, Yahoo, DropBox, MySpace, etc.)
5	**https://snusbase.com**	This site offers a paid search and API capability against what appears to be all the databases from other Databases.

ALL RIGHTS RESERVED

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WHAT CAN A USER LEGALLY DO WITH BREACH DATA

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

WHAT CAN A USER LEGALLY DO WITH BREACH DATA

There are many legal and ethical uses for breach data, which includes acting as a critical source for enabling OSINT investigations. There are several recommendations for responsibly using this information:

- Enable your own investigative efforts or OSINT trade craft;
- Support only current clients and services. Notifying prospective individuals or companies;
- Understand your company or unit's policies for collecting, securing and storing, and using this data ;
- Finding patterns in passwords or usernames, and other methodology or research interests;
- Being a security advisor or Professional of a company, you can randomly check company's published email addresses over these websites;

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

PROHABITED USE OF BREACH DATA

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ALL RIGHTS RESERVED

PROHABITED USE OF BREACH DATA

There are numerous challenges while assessing a data breach for individual or for a company becomes a serious issue for those countries where privacy is the concern.
Here are some list of limitation & challenges which may occur during the data breach analysis phase:

1. Reputation management is another strong concern since the general public is often uncomfortable with companies or government agencies collecting citizens' personal information (even publicly available);
2. If you are storing this data (particularly in a cloud environment), it is in your interest to take all necessary measures to comply with applicable data and privacy laws*;
3. Do not illegally profit from the breach data (i.e. cannot use it to commit another crime);
4. Do not sell breach data to third parties (enabling your own investigative capabilities as opposed to selling data for profit);
5. Do not, or induce others to, encourage or pay hostile actors to acquire this data;
6. Most people will not understand how you obtained the data, will likely be suspicious of what you are trying to do and could misinterpret your actions as blackmailing.

ALL RIGHTS RESERVED

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

THANK YOU

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.