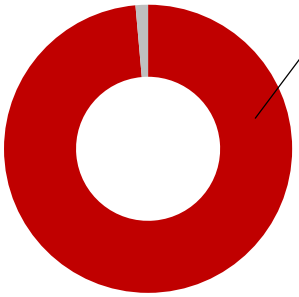
Soliton

Domain Data Leakage Assessment Report By Japan's Technology leader

How Secure is your Domain?
Get Soliton's vulnerability assessment report to assess where your data leakages are



98.9%

of domains have at least one breached account

*Based on all domains analyzed between July 2017~June 2018

Is your organization protected?

600+
Data Breach Incidents

Adobe
Twitter
LinkedIn
Yahoo!
Dropbox

20 Billion+
Compromised Credentials

e-mail
Password
Phone
Address
User ID

1,000+
Analyzed Domains in All Industries

Government
Automotive
BFSI
Retail
Manufacturing

Japan's trusted technology leader for over 40 years

Soliton®

See where your e-mail accounts, passwords and other credentials have been breached

NO	Breach Incident	Overview of Breaches	Country	Date	Total	Breaches	# of Accounts	Remarks
1	1.4 billion Credentials	In mid December 2017, 4iQ, a security intelligence company based in the US, issued a press release and warning titled "1.4 Billion Clear Text Credentials Discovered in a Single Database." At Soliton, we have unconvered these 1.4 billion credential records using open source intelligence (OSINT) – not via the dark web – and found these records were stored as in a file format rather than in a database, making it much easier to access and decipher to identify targets and their credentials for unauthorized login.	unknown	Dec 2017	1.1 B	Email addresses Passwords	84	Plaintext password
2	Anti Public	In December 2016, a huge list of email addresses and passwords in pairs appeared in a "combo list" commonly referred to as "Anti Public." The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", where attackers employ it in an attempt to identify other online systems where the account owner had reused the same password.	unknown	Dec 2016	458 M	Email addresses, Passwords	50	Plaintext password

NO	Breach Incident	Overview of Breaches	Country	Date	Total	Breaches	# of Accounts	Remarks
4	Exploit.In	In late 2016, a huge list of email address and password pairs appeared in a "combo list" commonly referred to as "Exploit.In." The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing," where attackers employ it in an attempt to identify other online systems where the account owner had reused the same password.	unknown	Dec 2016	593 M	Email addresses Passwords	33	Plaintext password
5	Collection #1	In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used in other breached services. Full details on	unknown	Jan 2019	2.7 B	Email addresses Passwords	28	Plaintext password

Deep dive into the accounts which have been breached, and identify potential future risks

Inferred name	Breached information						
	Email address	Breached websites	ID	Passwords			Note
				Plain	Encrypt	Hints	
a flores	aflores@xyz.com	1.4 billion Credentials		▯			
		Antipublic		▯			
		Collection #1		▯			
		Exploitin		▯			
		Linkedin			▯		
a meyer	ameyer@xyz.com	Adobe	▯		▯	▯	
a porter	aporter@xyz.com	1.4 billion Credentials		▯			
b bowman	bbowman@xyz.com	1.4 billion Credentials		▯			
b campbell	bcampbell@xyz.com	Dropbox			▯		

Soliton Systems
2635 North First Street, Suite 213
San Jose, CA 95134

Phone: 714-243-6121
E-mail: sales.us@solitonsys.com
URL: https://www.solitonsys.com/