





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	<b>1.4 billion Credentials</b>	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 uncovered 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	<b>84</b>	Plaintext password
2	<b>Anti Public</b>	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	<b>50</b>	Plaintext password

NO	Breach Incident	Overview of Breaches	Country	Date	Total	Breaches	# of Accounts	Remarks
4	<b>Exploit.In</b>	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	<b>33</b>	Plaintext password
5	<b>Collection #1</b>	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	<b>28</b>	Plaintext password



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

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