**Password Compromise**

On January 17, 2019, security professional Troy Hunt ​disclosed​ “Collection #1,” a data breach collection of 1,160,253,228 unique combinations of email addresses and corresponding passwords. A total of 772,904,991 unique email addresses and 21,222,975 unique passwords were discovered. Then, on January 31, PCWorld ​reported​ that researchers at the Hasso Plattner Institute discovered an additional 611 million credentials they attributed to the Collection #1 data breach.

The complete dump was analysed, which confirmed that many of the account credentials contained in Collection #1 are from a wide variety of previous data breaches, some of which are two to three years old, and may not contain newly compromised accounts. ​The Collection #1 database and its variations continue to be shared among dark web communities and incorporated in credential-stuffing attacks from various threat actors.

**1.​** ​**The links below are to articles that discuss the “Collection #1” data breach. Forbes: Collection 1 Breach -- How To Find Out If Your Password Has Been**

**Stolen**

**Troy Hunt: The 773 Million Record "Collection #1" Data Breach**

As you read through these, pay close attention to what information was compromised, number of records, and where they came from.

**2.​** ​**Answer the following questions regarding the attack itself:**

What is credential stuffing?

* Credential stuffing is a type of brute force attack that uses stolen credentials from another source. The most commonly used source violates a variety of online services. Greater values are put at risk by stolen credentials in situations when users have used the same credentials across many services. The BIG-IP can now detect similar attacks by using an authentication database that has previously been compromised. The identifiers are kept avoiding further disclosure in single-way, hashed usernames and passwords.

How were the clear text passwords obtained?

* The passwords' protective hashing had been compromised. This means they are straightforward to use because they are available in clear text rather than hashed, as they frequently are when websites are hijacked.

How can people find out if they were affected?

* You should visit Have I Been Pwned to find out if your password has been compromised, visit Pwned Passwords, a new feature on the site. This feature also encourages you to use strong passwords: if yours is published, it's safe to assume that others are, too, and your accounts could be easily stolen.

What is a good way to manage several passwords at once?

* A password manager is a secure vault where you may store all of your secrets (not just passwords; I also store credit card and banking information in mine), and its sole purpose is to keep them safe and secure.

What's the risk If your data is in there?

* If your password appears on the list, don't ignore it can be used in the previously disclosed credential stuffing attacks. lists that contain our email addresses and passwords are locked at more to see where else they can work. This strategy's success is reliant on users utilising the same credentials for many services.

What are some countermeasures that can be used to mitigate the risks of these credentials being used by threat actors?

* It's time to update your password policies. Passwords should be complex, such as a passage from a favourite book or a song lyric, and two-factor authentication should be used. At the same time, security experts do not rule out the use of analogy books to store your password if they are not maintained on or with your device. If you follow these steps, you should be able to avoid using the same password on many websites. If possible, start utilising a password manager to help you remember them. Having frequent password changes (every 30-60 days) and a password reuse policy can also be effective.