Issued 5/9/17

Over ONE Billion User Name and Password Combinations found on Web

In late 2016, a huge list of email address and password pairs appeared in two "combo lists" referred to as “Exploit.In" and “Anti Public”. The list contained Exploit List 593 million unique email addresses, many with multiple different passwords hacked from various online systems, and the Anti Public has 458 Million combinations . (It is not know how many duplicate emails are on both lists.) The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. It is also unclear how these lists got the information they have published.)

Credential stuffing is the automated injection of breached username/ password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.

This is a serious threat for a number of reasons:

1) It’s enormously effective due to the password reuse problem.
2) It’s hard for organizations to defend against because a successful "attack" is someone logging on with legitimate credentials.

3) It's very easily automated; you simply need software which will reproduce the logon process against a target website.
4) There are readily available tools and credential lists that enable anyone to try their hand at credential stuffing.

To find out if your credentials were on either of these lists go to: **https://haveibeenpwned.com** and enter your email address (or addresses if you have more than one). If you have been compromised, it is time to change your passwords on any accounts using that email. (And please don't use the same password for all your accounts.)