Hello [Client],

I am Rohan Taneja from Cyber Security Team – Goldman Sachs (Virtual Experience). I am here to report about the vulnerabilities figured in the credentials dump received. On reviewing the given document, we have found following analysis.

The type of hashing algorithm used to protect passwords is mainly MD5 (expected MD4 for uncracked credentials).

The security offered by this hashing method is not good enough for password protection. In modern day security MD5 is highly compromised since 2013. It provides 128-bit hash value for the input string.

In the event of data breach, few measures such as more enhanced cryptographic functions could be used to encrypt the stored credentials, an inhouse password strength checkers could be implemented when assigning password to the users, longer length of password should be used, and a modern salted cryptographic hash function could be implemented as mentioned earlier.

The organization should implement password policy that would prevent the use of generic word list passwords and would only allow unique, random generated, and complex passwords to their user accounts.

These are my insights for the policies. And from the data – 13 inputs were cracked using the online database – remaining 6 inputs of hash can also be looked up by reverse engineering the hash as MD5 is highly vulnerable due its length exploits by collision attacks.

Regards,

Rohan Taneja