Goldman Sachs

To: Dear Sir/Ma'am
From: Pablo Jimenez
CC: Forage Internship

While cracking all the leaked hashes, I found several vulnerabilities in your password policy and this memo determines all my findings and suggestions to improve your password policy.

Secure Hash Algorithm(SHA) and Message Digest(MD5) are the standard cryptographic hash functions to provide data security for authentication. It was easy to crack with Hashcat by using VMware and rockyou.txt wordlists via terminal. All passwords are compromised using MD5, which is a weaker hash algorithm and is prone to collisions. I would suggest that you use a much stronger password encryption mechanism to create hashes based on SHA.

After cracking the passwords, I found the following things about the organization password policy:

- Minimum password length is set to 6 and maximum password length is 9
- No specific requirements for creating passwords
- Users uses combination of words and letters

My recommendations for password policy are:

- Minimum password length to 10 or more
- Never reuse your passwords
- Use combinations of upper-case and lower-case letters, numbers, and special characters.
- Don't include username, full name, date of birth, and personal information when creating a password

- Train users to follow these policies to keep passwords safe