Respected Team,

I have analysed all the leaked passwords and have found lots of vulnerabilities which can easily expose the accounts to hacking threats. Here by I have listed all the insights of leaked passwords and some suggestions for the organisation's password policies.

After making all the analyses using Hashcat Tool and other hash identifiers like hashes.com, crackhash.com - it has been found that all the passwords contain MD5 hash function. This make the passwords weak and can easily be hacked.

Bare minimum requirement of standard cryptographic hash functions which are Secure Hash Algorithm (SHA) like SHA-256 and SHA-3 & Message Digest (MD5) should be use to maintain the security of passwords.

I would like to suggest some controls which should be implemented for making the cracking harder:

1. Setting a minimum length password rule.
2. Passwords should always contain special characters, Uppercase-Lowercase alphabets, numbers.
3. Password Salting concept and using strong hashing algorithm should be implemented.

It has been observed that there is no as such rule regarding the minimum length of the password to be used and no force over user for adding special characters in the password.

Kindly note that most of the passwords were generated with easy of keyboard setup – Like the series of set alphabet and characters on keyboard.

Hence, password policies should be updated keeping the below points in mind -

1. Password must be of minimum 8-10 characters.
2. Should not use common words.
3. Should not allow reusing the old passwords.
4. Should not let user to add series of numbers like 1234, 0000, abcd or wxyz etc.
5. Should showcase the strength of password using an external API.
6. Users should have warning message on screen for showing minimum requirement for designing any password.

Below is the list of the 19 hashcodes with only 13 cracked passwords. Remaining were not cracked. All the passwords have used MD5 algorithm as stated above.

Username	Hashcode	Cracked Password
experthead	e10adc3949ba59abbe56e057f20f883e	123456
interestec	25f9e794323b453885f5181f1b624d0b	123456789
ortspoon	d8578edf8458ce06fbc5bb76a58c5ca4	qwerty
reallychel	5f4dcc3b5aa765d61d8327deb882cf99	password
simmson56	96e79218965eb72c92a549dd5a330112	111111
bookma	25d55ad283aa400af464c76d713c07ad	12345678
popularkiya7	e99a18c428cb38d5f260853678922e03	abc123
eatingcake1994	fcea920f7412b5da7be0cf42b8c93759	1234567
heroanhart	7c6a180b36896a0a8c02787eeafb0e4c	password1
edi_tesla89	6c569aabbf7775ef8fc570e228c16b98	password!
liveltekah	3f230640b78d7e71ac5514e57935eb69	qazxsw
blikimore	917eb5e9d6d6bca820922a0c6f7cc28b	Pa$$word1
johnwick007	f6a0cb102c62879d397b12b62c092c06	bluered
flamesbria2001	9b3b269ad0a208090309f091b3aba9db	Not Found
oranolio	16ced47d3fc931483e24933665cded6d	Not Found
spuffyffet	1f5c5683982d7c3814d4d9e6d749b21e	Not Found
moodie	8d763385e0476ae208f21bc63956f748	Not Found
nabox	defebde7b6ab6f24d5824682a16c3ae4	Not Found
bandalls	bdda5f03128bcbdfa78d8934529048cf	Not Found

I hope the above clarification suffice the findings. Thank you.

Regards,

Shiwani Sabnis