Ne Tür Şifreler Kullanıyoruz ?

written by Mert SARICA | 13 January 2011

Geçtiğimiz günlerde yakın bir arkadaşımdan 34762 adet üyesi olan meşhur bir haber sitesine ait veritabanın yeraltı dünyasında elden ele gezdiğini öğrendim.

Hack edilen veritabanları ahlaksız korsanlar için oldukça değerlidir çünkü buradan elde ettikleri kişisel bilgiler sayesinde (e-posta, isim, soyad, şifre) bu kullanıcıların başka sistemler üzerinde (sosyal ağlar, e-posta sistemleri vb.) aynı şifreleri kullanıp kullanmadıklarını kontrol ederek bu kullanıcılara ait daha fazla bilgiye ulaşmaya çalışırlar. Bunun altında yatan amaç kişisel bilgilerin satılması ile elde edilecek kazançtır. İşte bu yüzden her sistemde farklı şifre kullanılması oldukça önemlidir.

Hack edilen veritabanları ayrıca ahlaklı korsanlar ve sistem yöneticileri içinde oldukça değerlidir. Mesela sistem yöneticileri bu veritabanlarında yer alan şifreleri analiz ederek tahmin edilmesi kolay olan şifreleri tespit edebilir ve yönettiği sistemlerde bu şifrelerin kullanılmasını yasaklayabilir. Bu yaklaşımın amacı bir nevi şifre kara listesi oluşturmaktır bu sayede şifre politikalarına rağmen zayıf şifre kullanmaya meyilli olan kullanıcıların bu şifreleri kullanması engellenebilir.

Ahlaklı korsanlar ise bu veritabanlarında yer alan bu şifreleri kendilerine güzel bir sözlük oluşturmak amacıyla kullanabilirler. Bu sözlük sayesinde izin alınmış hedef bir sisteme sızmak için gerçekleştirilen sözlük saldırılarının (dictionary attack) başarıya ulaşma ihtimali yükselir ve sistemdeki zayıf şifre kullanan kullanıcılar tespit edilerek olası bir ihlalin ve yaratacağı etkinin önüne geçilmiş olur. Peki ya aynı yöntemi ahlaksız korsanlarda izlerse ne olur ? Bu durumda herhangi bir sistem üzerinde zayıf şifre kullanan kullanıcıların hesapları kısa bir süre içinde art niyetli kişilerin kontrolüne geçer ve kullanıcılar için kabus dolu günler başlamış olur.

Bu veritabanı ile karşılaşınca en çok yurdum insanı güçlü şifre kullanımı konusunda ne kadar bilinçli sorusuna cevap aramak istedim ve grep, cat, sort, uniq, head, wc gibi basit metin araçları ile işe koyuldum.

Son kullanıcılar için güçlü şifre politikası büyük küçük harflerden, sayılardan, özel karakterlerden ve en az 8 karakterden oluşmalıdır düşüncesiyle bu politika ile uyumsuz olan şifreleri veritabanında aratmaya başladım.

Tekil (uniq) şifrelerin sayısı:

```
cat pass.txt | sort | uniq -ciu | wc -l
26123
```

En uzun şifrenin uzunluğu:

```
cat pass.txt | sort | uniq -ciu | wc -L
28
```

Sadece sayılardan oluşan 50 şifre:

```
grep -e “^[0-9]*$” pass.txt | sort | uniq -ic | sort /r | head -n 50
979 123456
103 111111
84 123123
81 000000
73 123456789
65 666666
58 12345678
56 112233
39 121212
38 14531453
32 123654
29 654321
29 19031903
28 159753
25 19051905
25 123321
24 313131
22 131313
21 1234567
20 19881988
20 19871987
20 112358
19 555555
19 212121
19 19891989
```

```
19 19071907
19 1123581321
19 101010
17 222222
17 19861986
17 19841984
17 12341234
16 102030
15 159357
15 147852
14 7777777
13 333333
13 19901990
12 987654321
12 987654
12 852456
12 353535
12 252525
12 19851985
12 19801980
12 159951
12 12344321
12 12121212
12 010203
12 00000000
```

Sadece sayılardan oluşan tekil (unique) şifrelerin sayısı:

```
grep -e “^[0-9]*$” pass.txt | sort | uniq -icu | wc -l
10842
```

Sadece harflerden oluşan 50 şifre (Türkçe karakterler hariç):

```
grep -e “^[a-zA-Z]*$” pass.txt | sort | uniq -ic | sort /r | head -n 50
115 (*sitenin adı sansürlendi*)
57 qwerty
47 sanane
41 istanbul
34 ankara
30 password
30 parola
```

30 asdasd
26 galatasaray
26 besiktas
25 Fenerbahce
21 deneme
19 cimbom
17 qazwsx
16 portakal
16 kartal
14 asdfgh
12 aaaaaa
11 unuttum
11 merhaba
10 zeynep
10 malatya
10 hebele
9 yagmur
9 qweasd
9 kelebek
9 kanarya
9 hacettepe
8 penguen
8 mustafa
8 karakartal
8 darkness
7 ultraslan
7 serdar
7 manyak
7 cancan
7 asdfghjk
7 anamur
6 trabzon
6 sananebe
6 metallica
6 marmara
6 kertenkele
6 karakter
6 hedehodo
6 emreemre

6 egemen
6 anadolu
6 alperen
5 zxcvbn

Sadece harflerden oluşan tekil (unique) şifrelerin sayısı (Türkçe karakterler hariç):
grep -e “^[a-zA-Z]*$” pass.txt | sort | uniq -icu | wc -l
6042

En çok kullanılan 50 şifre:
cat pass.txt | sort | uniq -dci | sort /r | head -n 50
979 123456
115 (*sitenin adı sansürlendi*)
103 111111
84 123123
81 000000
73 123456789
65 666666
58 12345678
57 qwerty
56 112233
47 sanane
41 istanbul
39 121212
38 14531453
34 ankara
32 123654
30 password
30 parola
30 asdasd
29 654321
29 19031903
28 159753
26 galatasaray
26 besiktas
25 fenerbahce
25 19051905
25 123321

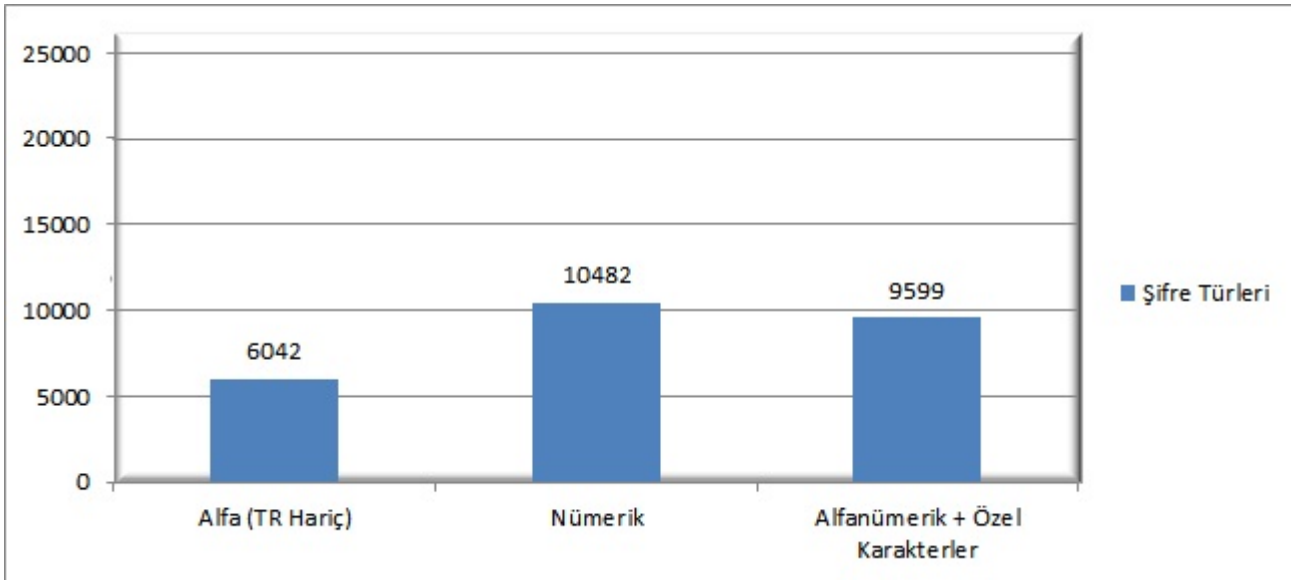
24 313131
24 1q2w3e
24 123qwe
22 bjk1903
22 131313
21 deneme
21 1q2w3e4r
21 1234567
20 19881988
20 19871987
20 112358
19 cimbom
19 555555
19 212121
19 19891989
19 19071907
19 1123581321
19 101010
18 qwe123
17 qazwsx
17 222222
17 19861986
17 19841984

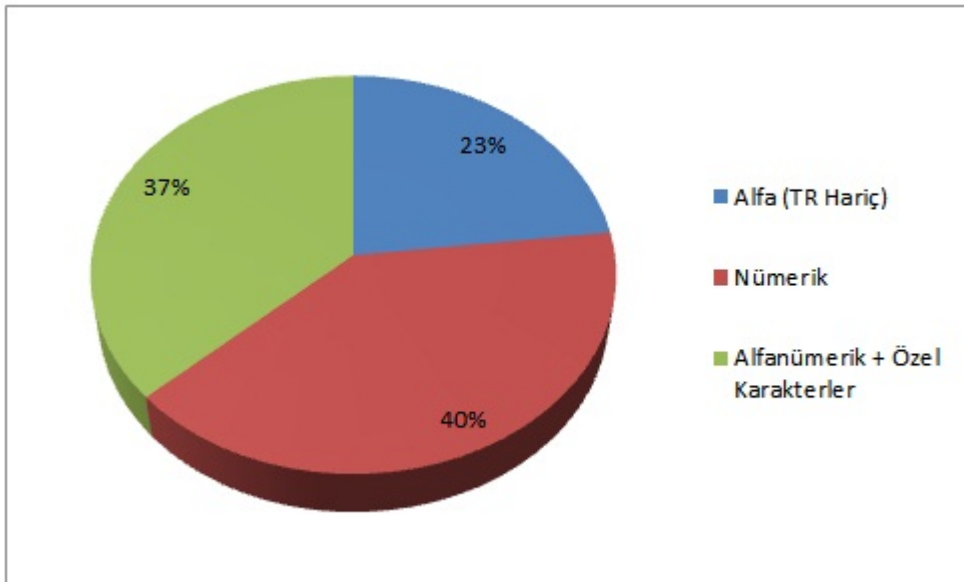
Hem harflerden hem de sayılardan oluşan 50 şifre (Türkçe karakterler hariç):

grep -e “^[a-zA-Z0-9]*$” pass.txt | sort | uniq -ic | sort /r | head -n 50

979 123456
115 (*sitenin adı sansürlendi*)
103 111111
84 123123
81 000000
73 123456789
65 666666
58 12345678
57 qwerty
56 112233
47 sanane
41 istanbul
39 121212

38 14531453
34 ankara
32 123654
30 password
30 parola
30 asdasd
29 654321
29 19031903
28 159753
26 galatasaray
26 besiktas
25 fenerbahce
25 19051905
25 123321
24 313131
24 1q2w3e
24 123qwe
22 bjk1903
22 131313
21 deneme
21 1q2w3e4r
21 1234567
20 19881988
20 19871987
20 112358
19 cimbom
19 555555
19 212121
19 19891989
19 19071907
19 1123581321
19 101010
18 qwe123
17 qazwsx
17 222222
17 19861986
17 19841984





En çok kullanılan şifrelere bakıldığında ve kullanılan şifrelerin %40'ının sayılardan %37'sinin sadece İngilizce harflerden oluştuğu düşünüldüğünde güçlü şifre kullanımında istenilen seviyede olduğumuzu söylemek biraz güç olur.

Art niyetli kişilerin şifrelerinizi tespit etmelerini zorlaştırmak için mutlaka ama mutlaka şifrenizde büyük ve küçük harflere, sayılara, özel karakterlere ($, !, ? vb.) ve en az 8 karakter uzunluğunda olmasına özen gösterin ve her platformda, sistemde farklı şifreler kullanmaya çalışın aksi durumda kişisel bilgilerinizin, hesaplarınızın ele geçmesiyle telafisi güç olan zor günler geçirebilirsiniz.

Sistem ve veritabanı yöneticilerine ise bu tür durumlara düşmemek ve kullanıcılarını zor durumda bırakmamaları için kullanıcılara ait şifreleri veritabanı üzerinde mutlaka ama mutlaka şifreli (encrypted) veya saltlanmış + hashlenmiş olarak saklamalarını şiddetle öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.