

Hackedin

written by Mert SARICA | 7 June 2012

Bildiğiniz üzere geçtiğimiz gün 150 milyondan fazla üyesi bulunan LinkedIn sosyal ağının hacklendiği, 6.46 milyon üyesine ait olduğu öne sürülen ve içinde SHA-1 ile hashlenmiş şifreleri barındıran dosyanın bir Rus sitesinde keşfedildiği ortaya çıktı. Benim gibi milyonlarca üye haberi duyar duymaz apar topar şifrelerini değiştirmek için zamanla yarışmaya başladı. Her ne kadar dosya içinde SHA-1 ile hashlenmiş şifreler dışında başka bir bilgi yer almamış olsa da LinkedIn'i hack eden art niyetli bilgisayar korsanlarının (black hat) başka hangi bilgileri ele geçirdiği bilinmiyor. (Her ne kadar şifremizi değiştirmiş olsakta SHA-1 ile hashlenmiş olan şifrelerin hangi zafiyetin istismar edilmesi ile ele geçirildiği bilinmediği için art niyetli bilgisayar korsanlarının tekrar bu bilgileri ele geçirip geçiremeyecekleri bilinmiyor bu nedenle olay netlik kazanana dek LinkedIn üyelerinin şifrelerini kendi güvenlikleri için gün aşırı değiştirmeleri yerinde olur.)

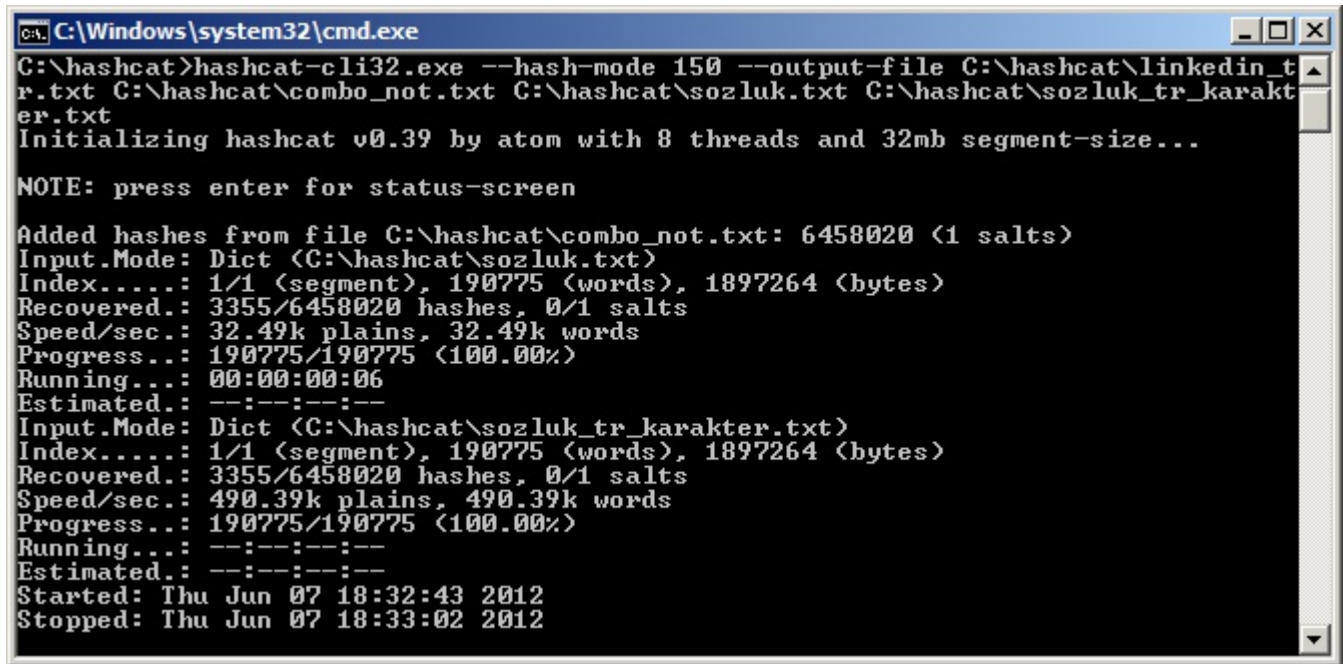
Bildiğiniz gibi art niyetli bilgisayar korsanlarının (black hat) bu bilgileri ele geçirdikten sonra yapacakları ilk iş SHA-1 ile hashlenmiş şifreleri orjinal yani okunabilir haline (password recovery) çevirmektir bu nedenle şifre seçerken sözlükte yer almayan kelimelerin kullanılması (oluşturulan şifrenin büyük ve küçük harf, özel karakter (\$, #, ? vs.) içermesi ve 8 haneden uzun olması tavsiye edilir) bu tür vakalarda çalınan, ele geçirilen şifrelerin okunaklı halini (clear text) art niyetli kişilerin eline geçmesini oldukça zorlaştırmaktadır. Art niyetli bilgisayar korsanlarının internetten temin ettikleri herhangi bir Türkçe sözlük ile hashlenmiş bu şifrelerin kaç tanesini orjinal haline çevirebileceklerini öğrenmek için aynı yöntemi izlemeye ve zayıf şifreleri tespit etmeye karar verdim.

Şifre kırma işlemi için hem hız hem de performans açısından başarılı bulduğum ve güvenlik testlerinde kullandığım hashcat aracını, sözlük dosyası olarakta 2010 yılında TDK Büyük Türkçe Sözlük'ten faydalanarak oluşturmuş olduğum hem Türkçe karakterleri içeren hem de içermeyen iki ayrı Türkçe sözlük dosyasından (dictionary file) faydalandım.

İşleme başlamadan önce SHA-1 ile hashlenmiş şifreleri içeren dosyayı incelediğimde 40 bayt (byte) olan SHA-1 hashlerinden (160 bit) bazılarının ilk 5 baytının 00000 olduğunu gördüm. Bunun sebebinin LinkedIn'i hackleyen art niyetli kişi veya kişilerin orjinal haline çevirebildikleri şifreleri bu

şekilde işaretlediği tahmin ediliyordu. 6.5 hashlenmiş şifrenin 3.5 milyonunun bu şekilde olması şifre kırma araçlarının sadece geriye kalan 3 milyon hash üzerinde şifre çevirme işlemini gerçekleştirebilmesi anlamına geliyordu çünkü 00000 ile başlayan bir hash bu araçlar tarafından tanınmadığı için aslında çöpten başka birşey değildi ancak dün akşam hashcat'in bu 5 haneyi de şifre çevirme işlemine dahil edebilen özel bir sürümü yayınladı.

Bu sürüm ile hashcat'in herhangi bir kuralından (attack modes) faydalanmayarak gerçekleştirmiş olduğum ilk testte aracın 6458020 hash'in 3355 tanesini (%0.05) başarıyla orijinali haline çevrilebildiğini gördüm.



```
C:\Windows\system32\cmd.exe
C:\hashcat>hashcat-cli32.exe --hash-mode 150 --output-file C:\hashcat\linkedin_tr.txt
r.txt C:\hashcat\combo_not.txt C:\hashcat\sozluk.txt C:\hashcat\sozluk_tr_karakt
er.txt
Initializing hashcat v0.39 by atom with 8 threads and 32mb segment-size...

NOTE: press enter for status-screen

Added hashes from file C:\hashcat\combo_not.txt: 6458020 (1 salts)
Input.Mode: Dict (C:\hashcat\sozluk.txt)
Index.....: 1/1 (segment), 190775 (words), 1897264 (bytes)
Recovered..: 3355/6458020 hashes, 0/1 salts
Speed/sec.: 32.49k plains, 32.49k words
Progress...: 190775/190775 (100.00%)
Running....: 00:00:00:06
Estimated.: ---:---:---:---
Input.Mode: Dict (C:\hashcat\sozluk_tr_karakter.txt)
Index.....: 1/1 (segment), 190775 (words), 1897264 (bytes)
Recovered..: 3355/6458020 hashes, 0/1 salts
Speed/sec.: 490.39k plains, 490.39k words
Progress...: 190775/190775 (100.00%)
Running....: ---:---:---:---
Estimated.: ---:---:---:---
Started: Thu Jun 07 18:32:43 2012
Stopped: Thu Jun 07 18:33:02 2012
```

```
C:\hashcat\linkedin_tr.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window 2
X

linkedin_tr.txt
1 00000926399ae73ef6948079549627b9265b0621: gardas
2 0000037f51e3517e781c00e96848658de1fbbf2: dalayarak
3 00000b9f978e58cb07fef7a4b3d36ed6d422b2: kefreem
4 000000dc23b335db8a3520f841b99e70663137ca: oktemer
5 000006e161e6bee2f14740099c4bee824792699: abrakadabra
6 00000828f6da8168882cc29a11cc204de197f576: musafir
7 00000cb580e8bb114e72d418d8538b13066d4afe: guduru
8 000005664cd7b0288244497994d0c78a87d64f6e: simile
9 0000053abb2adb214fb787b1c3da980ee176e00: uterus
10 0000072b980b06a39e90315dff30d8e258078a00: dokdok
11 000002497abf8b5b25accb0a172fb3f35e59ed7: kehlibar
12 000007906eb543aba41eaf2cd498d26d5add9de: oludeniz
13 0000013f1fd924489eaa6ccbdad7a40be253e6d: abrama
14 00000e9d781819275a51ba8f92f557a9f112d4f6: musaib
15 00000d3ddcf9994760ba195d0c3411c11668e036: gukguk
16 00000023101df495b386f1f690b7c5f0340c0312: simine
17 0000044106101fe1f6623eeca5e29307c8a332c1: utopie
18 000001c9ece9e3cc432fe9db33f82ce8a0ffbea: doktor
19 00000be9264d0f2b1272f6fcc333e1d1421677ee: kekule
20 e81fc2e65d78f70622eeed2a94258b34a6471a: omerhacili
21 0000068b5f953679c1b2277cacb8702590a370d: absent
22 00000a9b955582b50470fc35ff8271cf85d9515: muslim
23 00000fe562a3587adf37008dff6485a6ff5b153a: simsim
24 000006f2fe99de74862e3a6c4a69387b6c381c69: gulguli
25 000001f524b9bcc3d903a87afface50775d9a30c: uveitis
26 00000a7d112cb6cfad0f7aa84505ad4f016716a: dokucu
27 000008d64df5cfeda488697b6ea3f23049ae964a: kelaynak
28 0000037d581bd259c6b48be429d8790360934e10: odemis
29 000009f6c275d7485e7af424499d3b2448f84db6: absinth
30 0000001b8ebca47a8b6ba751e96020e2ed6afce9: muspet
31 000003cca0039dcl64637055a5a0ca5835ddb2c: simsiyah
32 0000088def38aa592ec770f09349d6e087ee894: gulnar
33 000008fae14bf759cb7b72c0f93d00bd6bfff74c: uyanik
34 00000cf526384c3b0e091e90bf417a17a285ae59: dolani
35 000006c94ebd02ad93312343bbcef0a2b833a760: kelebex
36 00000f485d72a48dfce0834940bf07753a8d26c9: onemsiy
37 000000262d6ad7006c2cadd90a4f8115865e164: aktuerya
38 000009c89024062fa2cb89060a624e662a309422: mustak
39 000002a225b110f16f63b14f6fffaebf015891af: simulator

Normal text file |length: 163526 |lines: 3356 |Ln: 3356 |Col: 1 |Sel: 0 |UNIX |ANSI |JMS
```

Combinator kuralından (sözlükte yer alan her bir kelimenin bir diğeriyle birleştirilerek de kullanılması) faydalananarak gerçekleştirmiş olduğum ikinci testte ise aracın 6458020 hash'in 11953 tanesini (%0.18) başarıyla orijinali haline çevrilebildiğini gördüm.

```
C:\Windows\system32\cmd.exe
C:\hashcat>hashcat-cli32.exe --hash-mode 150 --output-file C:\hashcat\linkedin_tr.txt --rules-file C:\hashcat\rules\combinator.rule C:\hashcat\combo_not.txt C:\hashcat\sozluk.txt C:\hashcat\sozluk_tr_karakter.txt
Initializing hashcat v0.39 by atom with 8 threads and 32mb segment-size...

NOTE: press enter for status-screen

Added hashes from file C:\hashcat\combo_not.txt: 6458020 (1 salts)
Added rules from file C:\hashcat\rules\combinator.rule: 40
Input.Mode: Dict (C:\hashcat\sozluk.txt)
Index.....: 1/1 (segment), 190775 (words), 1897264 (bytes)
Recovered..: 11953/6458020 hashes, 0/1 salts
Speed/sec.: 308.85k plains, 7.72k words
Progress...: 190775/190775 (100.00%)
Running....: 00:00:00:24
Estimated..: --:--:--:--
Input.Mode: Dict (C:\hashcat\sozluk_tr_karakter.txt)
Index.....: 1/1 (segment), 190775 (words), 1897264 (bytes)
Recovered..: 11953/6458020 hashes, 0/1 salts
Speed/sec.: 591.75k plains, 14.79k words
Progress...: 190775/190775 (100.00%)
Running....: 00:00:00:13
Estimated..: --:--:--:--
Started: Thu Jun 07 18:29:13 2012
Stopped: Thu Jun 07 18:30:05 2012
```

```
C:\hashcat\linkedin_tr.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window 2
X

linkedin_tr.txt
1 00000894deabd295af97fe38cea509665169a44e:gadar123
2 00000926399ae73ef6948079549627b9265b0621:gardas
3 00000033fc78770efc16bcdf3eb43d13011e5d99:geret1
4 00000eeb65c99d9b628796c3e690703f26f58ee1:golli123
5 000001aee83f70a2a64b578b408b6c44818a8947:gomsul
6 0000037f51a3517e781c00e96848658dee1fbbf2:dalyarak
7 0000001e8dbb32748f625a758448b8e783fd4ec3:gozer1
8 00000c2117fac16668334d396f9957dca8ff1109:aksel1
9 00000245b6195b9c7100caecb66b68ce5c75008d:keer123
10 00000f9ea1c5ab2df3d08da824d2d96263d324f6:gozer123
11 000007c275290cfe91691d7ea49e93ee92a6eebd:daml23
12 000005664cd7b0288244497994d0c78a87d64f9e:simile
13 00000c6fcfb36d746e777231cb295cb228fc4f4a:aksel2007
14 000000d1b0558e29164c4d878208ae211ec35c8:gudu123
15 00000b9f978e58c0b07fef7a4b3d36ed6fd422b2:kefrem
16 0000082f6da8168882cc29a11cc204de197f576:musafir
17 000005ab2c16258aa379483672d1dc6c52a6a04d:ok2008
18 0000016dc714679cc9c6bd07673cc4a97e225bfb:usda2008
19 0000095d334fbb134c810729eb94a4f5ca590a49:abovet
20 00000c7d23a34896bc108873871b4b3974a45692:gudu2007
21 000008def5eb909341e132c1bdcba8daa4654661:doha123
22 000006bf622ef93b0a211cd0fd028dfdcf7e39e:user123
23 000008854c6264de8793979dbbd3ace0288c7030:okok123
24 00000a4d0001b8c4728173462da6de75d3c86b21:simsi1
25 0000021769eafdf73e6eda4e1afe0b0f3d174abd:abril1
26 00000cfc8efa0bbf7de62c6abe567e8841d2540:kehlxer
27 00000e9d781819275a51ba8f92f557a9f112d46f:musaib
28 00000640538c8ac8035c4960a8eeceaa011e4eb0:doha2008
29 00000ddae9e7e0859dedc557605cd9470dd46c06:user2007
30 00000cb580e8bb114e72d418d8538b1306d4afe:guduru
31 00000023101df495b386f1f690b7c5f0340c0312:simine
32 0000003d635d1e228dec45dc037859726da40cc5:abril2008
33 0000028497ebf8b5b25accb0a172fb3f35e59ed7:kehlibar
34 0000072647a04799c16399e53df68f072efbc878:doha2009
35 000000dc23b335db8a3520f841b99e70663137ca:oktemer
36 000009c33f410fb5707b2ae199d116ef38662b93:ustal23
37 000003f34c88a7a696fed84353ff471c6f3881533d1:abral23
38 00000a9b95558c2b50470fc35ff8271cf85d9515:muslum
39 00000e92c05bdac3a7aa60e1180efb4b3bf0e66a:dok123

Normal text file |length : 585879 |lines : 11954 |Ln : 3337 |Col : 18 |Sel : 0 |UNIX |ANSI |INS
```

Sözlükte yer alan basit kelimelerin şifre olarak kullanılması durumunda şifrelerin art niyetli bilgisayar korsanları tarafından çok kısa sürede internetten temin edilebilen sözlükler ile rahatlıkla kırılabileceğini hiçbir zaman unutmayın ve olabildiğince güçlü şifreler (oluşturulan şifrenin büyük ve küçük harf, özel karakter (\$, #, ? vs.) içermesi ve 8 haneden uzun olması) kullanmaya gayret edin.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim...