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.)

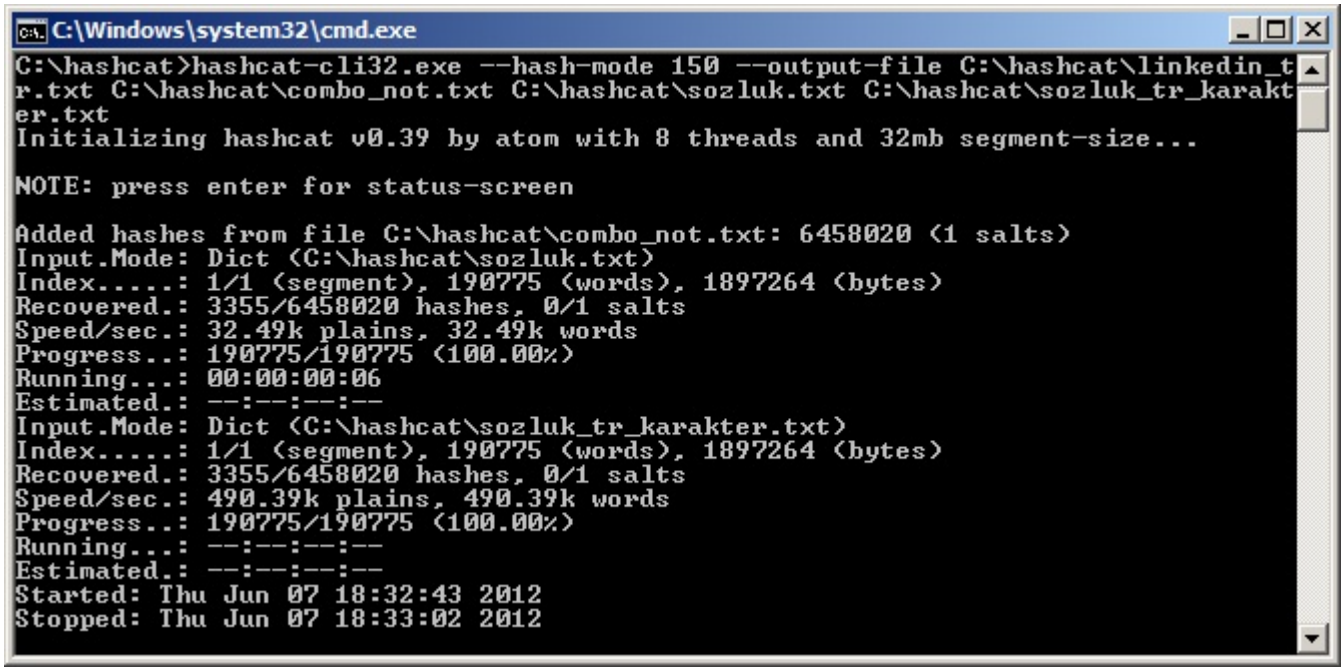
Bildiğiniz gibi art niyetli bilgisayar korsanlarının (black hat) bu bilgileri ele geçirdikten sonra yapacakları ilk iş SHA-1 ile hashlenmiş şifreleri orjinal yani okunabilir haline (password recovery) çevirmektir bu nedenle şifre seçerken sözlükte yer almayan kelimelerin kullanılması (oluşturulan şifrenin 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.

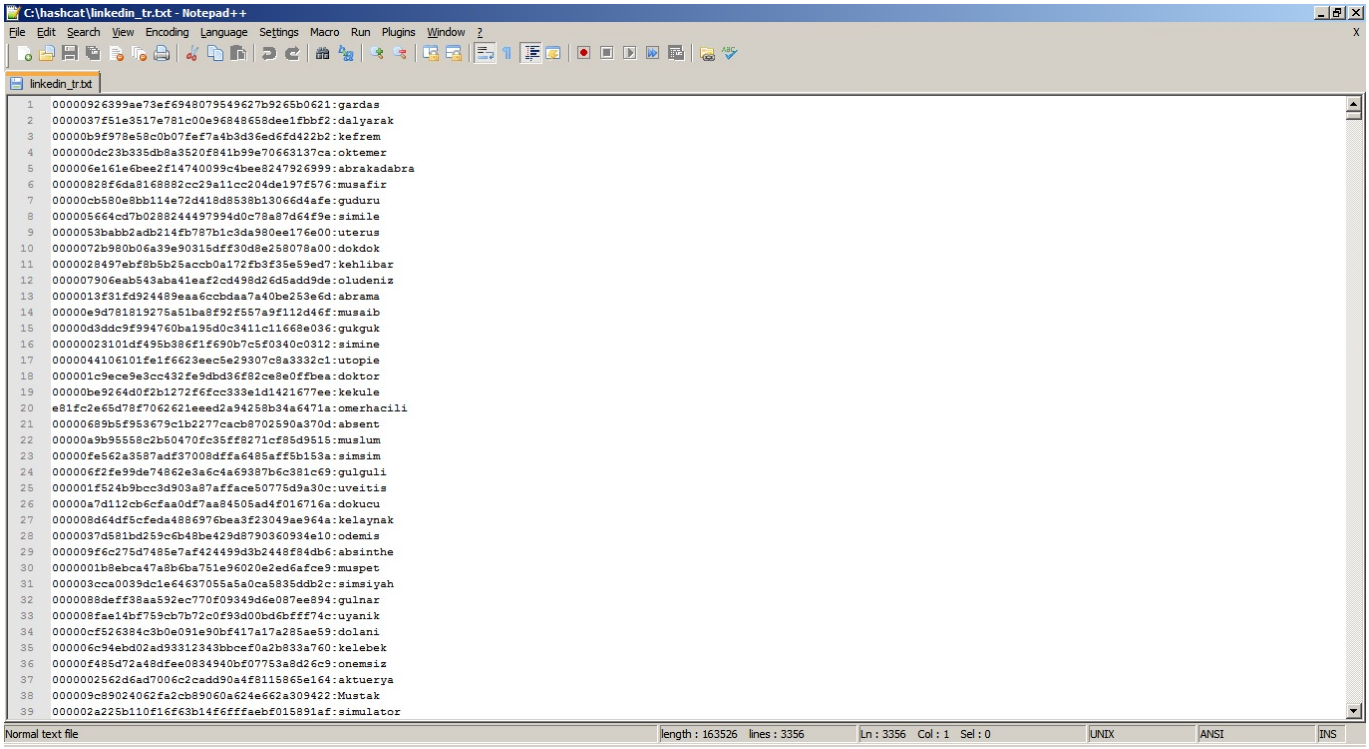
Şifre kırma işlemi için hem hız hem de performans açısından başarılı bulduğum ve güvenlik testlerinde kullandığım hashcat aracını, sözlük dosyası olarakta 2010 yılında TDK Büyük Türkçe Sözlük'ten faydalanarak oluşturmuş olduğum hem Türkçe karakterleri içeren hem de içermeyen iki ayrı Türkçe sözlük dosyasından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

İşleme başlamadan önce SHA-1 ile hashlenmiş şifreleri içeren dosyayı incelendiğimde 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

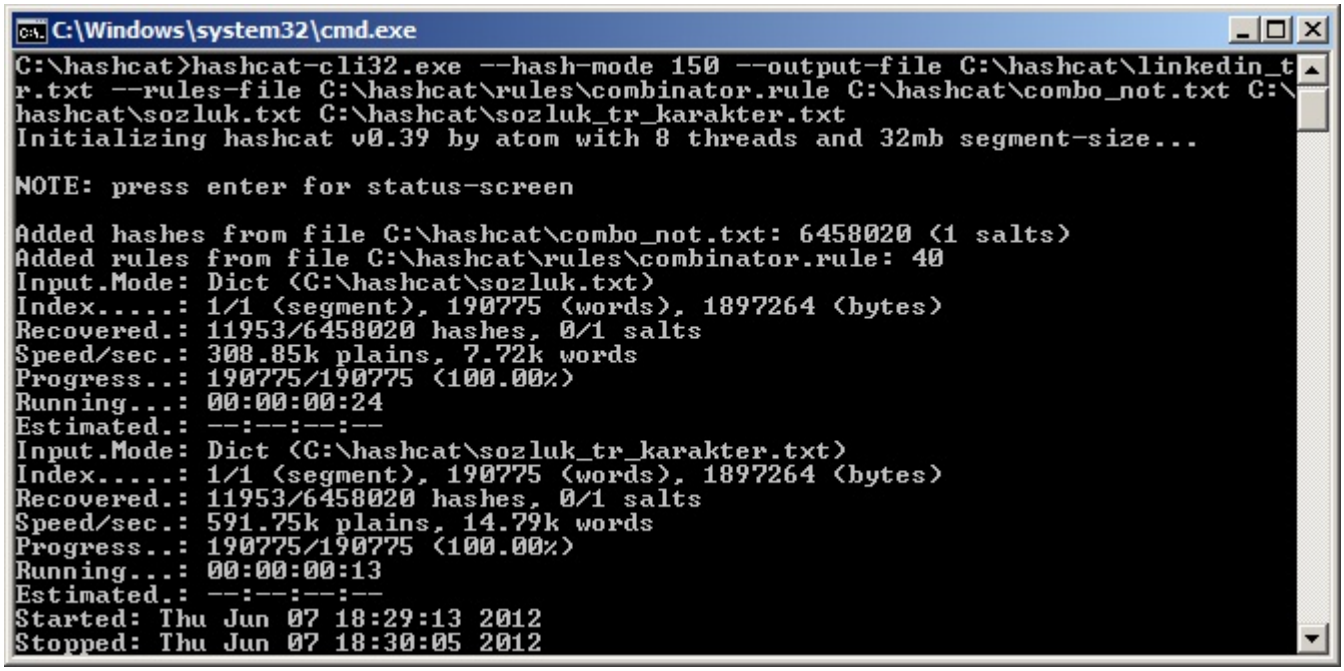
şekilde işaretlediği tahmin ediliyordu. 6.5 hashlenmiş şifrenin 3.5 milyonunun bu şekilde olması şifre kırma araçlarının sadece geriye kalan 3 milyon hash üzerinde şifre çevirme işlemini gerçekleştirebilmesi anlamına geliyordu çünkü 00000 ile başlayan bir hash bu araçlar tarafından tanınamadığı için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

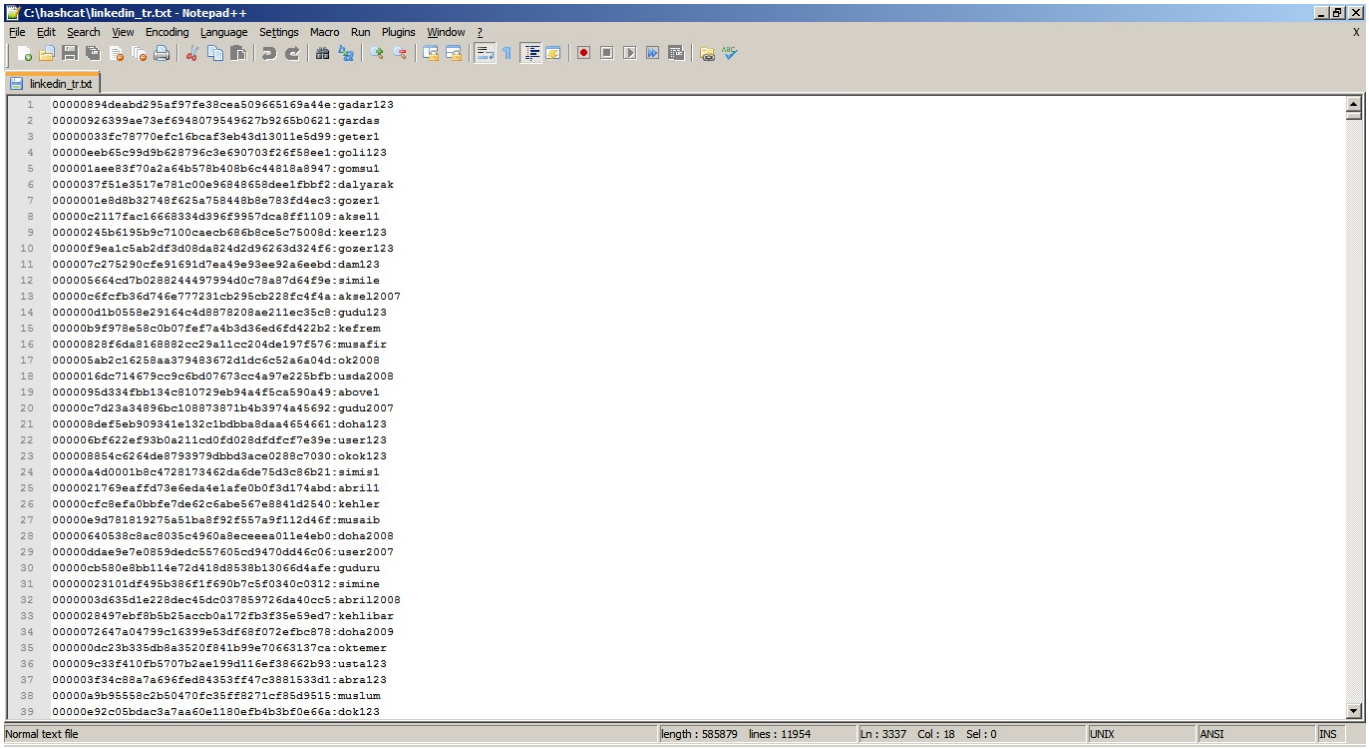
Bu sürüm ile hashcat'in herhangi bir kuralından (attack modes) faydalanmayarak gerçekleştirmiş olduğum ilk testte aracın 6458020 hash'in 3355 tanesini (%0.05) başarıyla orjinali haline çevrilebildiğini gördüm.





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





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…