



ASAL FAKTÖRLER

RSA SecurID ve Lockheed Martin

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Son birkaç aydır, casus romanlarına ait gibi gözükten olay ve haberler güvenlik dünyasını etkiledi. Önce Mart ayı ortalarında, RSA şirketinin yeni sahibi EMC şirketi ileri düzeyli bir siber saldırıya uğradıklarını ve saldırının RSA SecurID denilen iki-faktörlü donanım anahtarlarının (token) altyapısını hedeflediğini ve bazı bilgilerin çalındığını açıkladı. Türkiye’de de kullanılan bu anahtarlar, üzerindeki minik düğmeye basıldığında kullanıcı için 6-8 rakamlı bir sayı üretiyor; kullanıcı da bu sayıyı şirket bilgisayarlarına veya internet bankacılık hesabına girerken parola olarak kullanıyor. Sunucu ile senkronize olan bu sayılar dizisi, böylece sunucunun bu anahtarın sizde olduğuna emin olmasını sağlayarak, size erişim hakkı vermesini sağlıyor. Üretilen sayılar, genellikle bir önceki kullanımdaki sayı veya anın zaman bilgisi (gün-saat-dakika) gibi bilgileri bir blok şifreleme algoritması ile şifreleyerek elde edilmekte. RSA şirketi bir bildiri yayınlayıp, müşterilerimiz bundan etkilenmedi, dedi. Ancak, böyle düşünmeyenler çok. Eğer, saldırıyı yapan kişiler ve kurum, SecurID şifreleme anahtarını elde etmişse, bundan en azından belirli bir grup SecurID kullanıcıları etkilenecektir.

Bu olaylar, Mart ve Nisan aylarındaydı. Herkes hepsi bu kadarmış, diye düşünürken, 28 Mayıs günü, ABD’nin en prestijli savunma şirketlerinden Lockheed Martin, çok ciddi bir saldırıya uğradıklarını, ancak hızla hareket ederek, sistemlerinin güvenliğini sağladıklarını açıkladılar (herhalde, sistemleri devre dışı bıraktık demek istiyorlar). Gerçekten de ciddi bir saldırı olduğu belli ama, ABD’deki savunma şirketleri nerdeyse her hafta böyle şeylerle meşguller. Burada ilginç olan şey: adının yazılmasını istemeyen bir görevli, saldırının sahtesi yapılmış RSA SecurID anahtarlarıyla login olan (veya olmaya çalışan) kişiler tarafından yapıldığını belirtti.

Lockheed Martin sistemlerinde, savunma bakanlığına ait çok değerli bilgiler olduğunu sanılıyor. Küçümsenecek bir olay, basit hacker saldırısı olmadığı belli. Gördüğünüz gibi, Mart ve Nisan aylarındaki EMC/RSA saldırısını alıp, Mayıs ve Haziran aylarındaki Lockheed Martin saldırısına iliştiyorsanız, güzel bir John Le Carre romanı ortaya çıkabilir!