

## Ekşi sözlük, inci sözlük hacklendi mi ? nasıl hacklendi

Merhabalar arkadaşlar,

Daha önce bildiğiniz gibi güvenlik, sosyal mühendislik üzerine birkaç yazım olmuştu. Şimdi bunları sentezleyip, güncel bir olay üzerinden örneklemeye çalışıcam.

Bugün yani 28 Temmuz 2013 tarihinde ekşi sözlük, inci sözlük ve birkaç tane daha sözlük ve site hacklendi.

Sosyal medyanın aktif olarak takip edildiği siteler olduğu için de çoğu kişi tarafından far edilip, önemsendi.

### Peki ekşi sözlük, inci sözlük nasıl hacklendi?

Kimi zaman güvenlik uğruna ne kadar önlem alırsanız alın, sizin için yeterli olmaz. Bildiğiniz gibi daha önce [burada](#) işlemin yazılımsal güvenliğini sağlayan bir döküman, [burada](#) ise sitemin insan kaynaklı kısımlarına alınabilecek önlemleri görmüştük ama bunlar n yazık ki yeterli kalmıyor.

Bu faktörlerin dışında hostinginizin bulunduğu sunucu, hatta sunucunuzun bağlı bulunduğu datacenter'ın bile yeteri kadar güvenlik önlemi almış olması MITM gibi ataklara karşı kendini koruyor olması gerekmekte.

Gelelim bu sitelerin nasıl hacklendiğine.

Öncelikli olarak sistemde herhangi bir deface durumu yok, yani kodlara müdahalede bulunulmamış, sunucuya sızılma durumu da yok bu durumda geriye tek bir ihtimal kalıyor bu da domain.

Domaine ne gibi şeyler yapılabilir ?

Örneğin ekşi sözlüğün domainine whois çektiğinizde gkg.net adında bir firmadan alındığını görebilirsiniz. Bu firmanın ne kadar güvenli olduğu tartışılır. Ekşi sözlük kalitesindeki bir firmanın tercih etmemesi gereken bir firma olduğu ise zaten ortada.

Bu tür firmalarda bildiğiniz gibi destek sayfası bulunmakta. Muhtemelen saldırganlar ilgili firmanın yetkililerine veya çalışanlarına keylogger yedirerek panel bilgilerine ulaştılar. Daha sonra ise buradan

domainin name server bilgilerini deęiřtirdiler.

Normalde ekři sözlüğün buna karşı yapabilecek pek bir řeyi yok gibi gözüküyor ama asıl sorun burada başlıyor. Aksine ekři sözlüğün bu kadar önemli bir konuda, bu kadar önemsiz bir tercih yapmaması gerekiyordu.

Bugüne kadar bu yöntemle nic.tr, namecheap, register.com, publicdomainregistry ve bir çok firmaya sızılıp çok büyük firmalar hacklendi. Bu tür durumlardan genelde sağ çıkan firma ise godaddy oldu.

Bugüne kadar bildiğim kadarıyla atlattığı büyük bir sosyal mühendislik zaafı veya güvenlik zaafı bulunmuyor.

Şu anda ekři sözlüğün hala gkg.net'i kullandığını göz önünde bulundurursak bu tekrar hacklenebileceęi anlamına geliyor.

Mustafa Erdinç ZORBA

**28 Tem. 2013**

[info@merdincz.com](mailto:info@merdincz.com)

[www.merdincz.com](http://www.merdincz.com)