Siber Saldırıya Uğramak

ABD, Almanya, Belçika, Kolombiya, Polonya, Kosta Rika, Bulgaristan, Makedonya, Romanya, Rusya, Sırbistan, Kore, İran, İsrail, Hindistan, Tayvan, Filipinler, Ukrayna, Suudi Arabistan ve tabii ki *Türkiye.* Bu ülkelerden, âcizane web siteme sayısız ziyaretler yapılmış. Ama meraktan veya iyi niyetten değil, siteyi hack etmek (ele geçirmek) için!

Kendi halinde yazılar yazıp projelerini paylaşan, ticari ve politik bir mücadele içinde olmayıp, kişi ve kurumlara karşı tehdit sayılabilecek bir faaliyeti de bulunmayan birisine ait web sitesinin ısrarla çökertilmek istenmesi çok tuhaf ve hastalıklı bir durum. Ülkelerin listesinden de görebileceğiniz gibi küresel bir yozlaşmayı da gösteriyor.

Siteyi wordpress platformuna taşıyıp, daha aktif kullanmaya başladıktan sonra, tuhaf kilitlenmeler ve yavaşlıklar yaşamaya başladım. Safiyane bir şekilde, hosting hizmetini aldığım yerle ilgili teknik sorunlar olabileceğini düşünüyordum. Sonrasında güvenlik eklentisini de yükleyip, raporlar almaya başlayınca durum net olarak anlaşıldı: Düzenli olarak saldırı altında kalıyormuşuz!?

Saldıranların yapmaya çalıştığı şey: wordpress site yönetim panelinden erişim sağlayarak siteyi ele geçirmek. Kullanıcı adı olarak en çok denenen isimlerde şunlar: ***admin, administrator, user, test, sysadmin, support, root, qwerty, aaa, manager, ercanozcelik***. Bu isimleri özellikle yazdım ki, site yönetiminde bulunanlar yaygın isim ve

şifreleri kullanmaktan kaçınsın diye. Aynı IP adresinden yüzlerce defa "***admin***" olarak girmeye çalışmak patolojik bir durum, ama siteyi yavaşlatarak zarar da veriyor. Böyle ısrarlı vatandaşları görünce, 2 denemeden sonra yanlış kullanıcı adı ve şifre girilen IP adreslerini bloke edecek şekilde güvenlik ayarlarını güncelledim. Israrla denemeye devam edip bloke olan IP bilgileri mail raporu olarak bana da geliyor. Günlük ortalama 20 civarında mail geliyordu. Bir kaç gün boyunca 50-55'i bulduğu da oldu. Artık daha az geliyor çok şükür. Bu arada güvenlik eklentisinin üreticisi de rapor başlığı altında "böyle gitmez, tek tek IP adreslerini bloke edeceğine saldırıyı yapan ülkeyi komple bloke edebilirsin ama bunun içinde paralı eklentiyi alman lazım" mealinde reklam içeren mailler de gönderiyor. Ama başarılı çalışmalarından dolayı hoşgörü ile katlanıp idare ediyorum.

Bu yazıyı yazmadan hemen önce tekrar kontrol ederek ülke isimlerini almıştım. Dikkatimi çeken bir başka bilgi de şu oldu: "IP's who were recently throttled for accessing the site too frequently." (Mealen: Siteye son zamanlarda en çok saldıran IP'lerin kimdir, neredendir bilgisi) bölümü altında yazan ülkenin adı: İsrail. Hamaset edebiyatı yapacak değilim ama kısaca; Rabbim zalimlere fırsat vermesin, bizlere de şuur ve birlik versin diyorum. İçimizdeki İsrail hayranlarının kulakları çınlasın!

Bilişimle ilgilenen birisi olsam da, tahminlerimin ötesinde bir durumu yaşamış bulunuyorum. Web siteleri; Lamer tipinde özenti saldırılar yapanlardan, profesyonel Hacker ataklarına kadar 24 saat tehdit ve tehlike altında bulunuyor. Kişisel verilerin, şirket bilgilerinin, kamuya özel dataların tamamının çıkar amaçlı veya politik nitelikte saldırılara açık şekilde durması söz konusudur. Hiç bir şey olmasa bile, zombileşmiş site ve sunucular oluşturup, buralardan saldırılarına devam etmek istiyorlar. Bunları önlemek için: Bilgi güvenliği kurallarına titizlikle riayet etmek, site ve eklentilerini güncel tutmak, sağlıklı çalışan güvenlik yazılım ve sistemlerini kurmak gerekir.

Bütün bilişimci dostlarıma siber saldırısız günler dilerim…