

Ağ Güvenliği Akademisi #22 – Neden WEB Sitesi Güvenliği?

Ar. Gör. Enis Karaarslan,

Ege Üniversitesi Kampüs Network Yöneticisi

Günümüzde World Wide Web (WWW), güncel ve doğru bilgiyi insanlara ulaştırmak için en kolay ve en etkin yöntem olarak karşımıza çıkmakta. Kurulan bir web sunucusu ve içine hazırlanan site içeriği üzerinden, kurumunuz hakkında bilgiyi sunabilir ve ticaret yapabilirsiniz. Bu kolaylık sonunda, birçok ağ cihazı, 3G cep telefonları, UPS, kamera ve hatta çok ilginç birçok cihazın da üzerlerinde web sunucusu gelmeye başlamıştır.


Web servisleri, doğaları gereği kendilerine gelen http isteklerini karşılamak zorundadır. Web sunucularına gelen http istekleri, geleneksel ağ güvenlik duvarları (firewall) tarafından incelenmemektedir. Bu istekler içerisinde olabilecek saldırı kodları, http istekleri içinde gömülmüş olacaklarından geleneksel yöntemlerle tespit edilemezler. Bu yazıda bu konuya giriş yapacağız ve sonraki sayılarda saldırı ve savunma yöntemlerine de değinmeye çalışacağız.

Web sitesi saldırıları (web defacement) her geçen gün artıyor. Zone-h'in (<http://www.zone-h.org>) araştırmasına göre, 2004 senesinde web saldırıları 2003'e göre %36 arttı. Bu artışın 2005 ve 2006'da daha büyük oranlarda olduğunu tahmin ediyoruz. CSI/FBI'in araştırmasına göre (Computer Crime and Security Survey -2005) göre, katılanların %95'i 2005 senesinde 10'dan fazla web sitesi vakası yaşamış. Bu artışın asıl nedeninin, web sitesi güvenliğinin yeterince ciddiye alınmaması olduğunu düşünüyorum. Öncelikle web siteleri hızlı bir şekilde hazırlanıp sunulmaktadır. Özellikle forum, hazır web portal yazılımları; dinamik içerik sağlamak için veritabanı desteği sağlayan uygulama kodları (php, asp, jsp, cgi ... vb) web sitesinin en zayıf halkalarını oluşturuyorlar. Tabii ki bu siteler hazırlanırken hiçbir güvenlik kontrolünün yapılmadığını, kodlarda kullanıcıdan girdi alınan kısımlarda, alınan verinin hiç kontrol edilmediğini gözlemliyoruz. Saldırgan tarafından kodlara kasıtlı verilen değişik girdiler sonucunda hata sonuçlarının da direkt sayfaya basılması, saldırgana bilgi sağlamaktadır.

Büyük kurumsal ağlarda, sunucuların ve üzerlerinde çalışan uygulamaların sayısının artması ile sorunun arttığı gözlemlenmektedir. Bu tür sistemlerde en büyük sorunun, bu büyük ağlardaki hangi sistemin üzerinde ne çalıştığının tam olarak bilinmemesi olduğunu düşünüyorum. Bu büyük ağlarda, sunucuların hepsinin zamanında patch'lenmesi, log'ların takip edilmesi, uygulamaların kontrol edilmesi her zaman mümkün olamamaktadır. Bu sunucuların farklı kişiler tarafından yönetildiği durumlarda, idari sorunlar da olabilmektedir.

Internet'in haşarı çocukları, bazen hacker, bazen saldırgan(attacker), çoğu zaman lamer (sözde hacker) sitelerin bu açıklarını kullanarak ana sayfalarını değiştiriyorlar veya veritabanını ele geçiriyorlar. Bunun birçok nedeni ve sonucu olabilir, sonuçta yazı dizimizde daha önce bunun çeşitli nedenlerinden söz etmiştik. Saldırı sonrasında, işin raconu icabı, bir şekilde bu bilginin paylaşılması gerekir. Bu önceleri hacker siteleri ve forumları olmaktadır ama son zamanlarda bu paylaşım ortamı "Saldırı/Güvenlik haber merkezleri" diyebileceğimiz ilginç portallara yönelmiş durumda. Bu konuda Zone-h

(<http://www.zone-h.org>) ele geçirilen sitenin o anki ekran görüntüsünün sergilendiği bir portal ve saldırılar hakkında istatistiksel veriler tutması açısından bu konuda mükemmel bir referans noktası olmayı sürdürüyor. Saldırılan sistemin bilgileri, saldırıyı gerçekleştiren saldırganın lakabı ve hangi amaçla (politik, eğlence ...vb) bu saldırıyı yaptığı da sisteme girilmektedir.




zone-h
warfare

UNITED NATIONS AND SONY HACKED BY TURKISH

CRACKER III SUPPORT OF THE MUSLIM CYBER-JIHAD

User Rating: ●●●●● / 235

Written by Roberto Preatoni
Tuesday, 15 August 2006



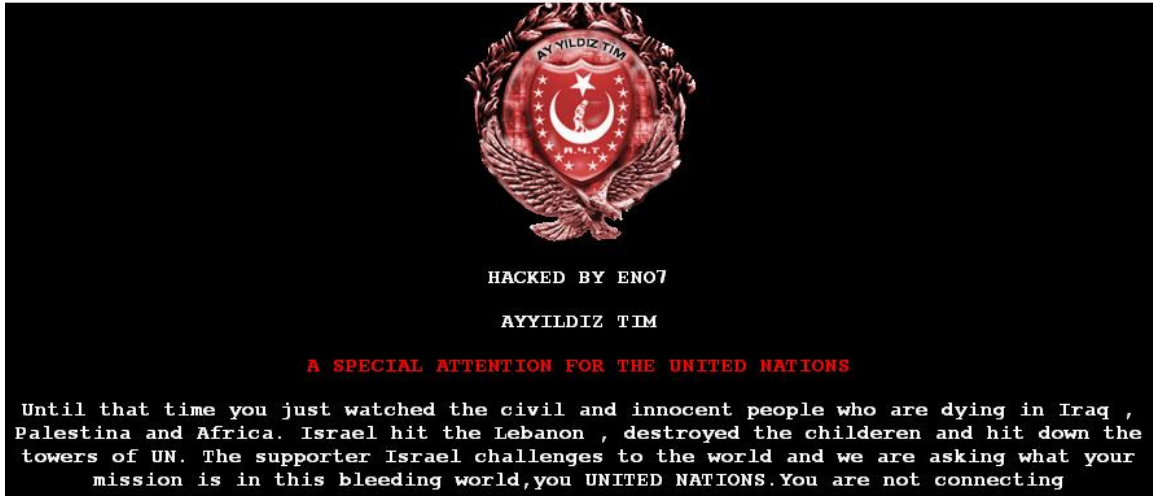
A few hours after the United Nations voted the resolution for the Lebanon peace keeping forces, the United Nation and Sony Philippines websites have been compromised by Turkish attackers Eno7, apparently in protest for the current Middle-East situation.

In the same defacements it is also announced an international crackers coalition featuring, for the first time ever, crackers from Cuba.

Mirror of the defaced site can be viewed [here](#)

The website has been defaced on a secondary page (currently under reconstruction), a typical Turkish logo appearing on the page followed by an English language statement (a bit sluggish as usual) reporting a political statement...

Mirror saved on: 2006/08/14 15:07		
Defacer: eno7	Domain: http://www.un.org/docs/ecosoc/documents.asp	IP address: 157.150.195.10
System: NetBSDOpenBSD	Web server: Apache	Attacker stats



Türkiye'den bir grubun, Gri Şapka (<http://www.grisapka.org>) adresinde de, Türkiye'deki web sitesi saldırıları ve hatta nasıl yapıldığına dair video görüntüleri bulunmakta. Türk Ceza Kanunu (TCK) uyarılarından sonra bu videoları sitelerinde barındırmamaya karar veren portal, bundan sonra sadece link vermekle yetinecek. Web sitesi güvenliği hakkında yazdıkları yazı gerçekten de üzerinde düşünölmeye değer:

Bilişim Güvenliği Neye Benzer ?

Bilişim güvenliği, güvenli seyahat etmeye benzer. Bir portal sahibi iseniz veya bir hosting firmanız var ise müşterileriniz veya kullanıcılarınız yolculara, siteniz otobüse, siz ise şoföre benzersiniz. Otobüsünüzü servise sokmazsanız, her koltuğa emniyet kemeri koymazsanız, bir gün freni patlarsa veya trafik canavarına rastlayıp kaza yaparsa, gerekli tedbirleri almadığınız için sizin ve yolcularınızın kazadan kurtulma şansı olmayabilir. Peki bu durumda tedbir almayan şoför mü hatalıdır? Otobüs şoförünü tedbir almaya zorlatmayan yolcular ve yasalar mı hatalıdır? Emniyet kemeri takmayan yolcular mı hatalıdır? Hatalı sollama yapan trafik canavarı mı hatalıdır? Yoksa kıymeti bilinmeyen canları almaya gelen Azrail mi hatalıdır? Azrail lütfedip ayağınıza kadar gelmişse mutlaka bir yerlerde birileri hata yapmıştır.

Sitemizde yayınlanan dosyalar nedeniyle bir çok kişi serzenişte bulunmakta ancak öz Türkçe ile tekrar ve tekrar hatırlatıyoruz, biz bir hack grubu değiliz, biz sitemizde rumuzlarıyla birlikte yayınlanan dosyaların sahibi değiliz. Biz, bize gönderilen haberleri, dosyaları, videoları yüzlerce kişiyle paylaşan kimi zaman sağduyunuz, kimi zaman eğitimciniz, kimi zaman ise kabuslarınızdaki canavarlarız.

(Kaynak: <http://www.grisapka.org>)

Sonuçta bu tür saldırıları yapmak dünyanın hiçbir yerinde yasal değildir. Zone-h, her ne kadar bu tür olayları destekliyor gibi gözükse de, sayfalarında bunun suç olduğunu da hatırlatmaktadır. "Hacker olarak tanınayım, sonra güvenlik sektörüne girerim" mantığının ise yanlış bir yol olduğunu hatırlatmakta yarar var.

Adalet Bakanlıđı'nın biliřim suçlarına iliřkin hazırladıđı kanun tasarısında, bilgisayar korsanlarına 2 yıldan 5 yıla kadar hapis ve adli para cezası verilmesi öngörölüyor. İlk zamanlarda uygulanmasında çeřitli aksilikler/anlařmazlıklar yařanabilir ama bu konuda çalıřmalara bařlanmış olması da çok önemli bir bařlangıçtır. ULAK-CSIRT (<http://csirt.ulakbim.gov.tr>) olarak bu hukuksal düzenlemeleri bizzat yakından takip ediyoruz ve bu hukuksal durum hakkında da önümüzdeki sayılarda sizi bilgilendirmeye çalıřacađız.

Kurumlar, bu tür web siteleri saldırıları sonucunda ciddi itibar kaybına uğramaktadır. Web üzerinden ticaret yapan kurumlar, veritabanlarının ele geçirilmesi durumunda ciddi ticari kayıplar yařayabilirler. Kullanıcıların kiřisel bilgilerinin ve kredi kartı bilgilerinin çalınması durumunda müřterileri ciddi sorun yařayabilir, müřteriler bu konuda yasal haklarını arama yoluna gidebilirler. Kurumlar bu tür durumları müřterilerinden saklama durumuna gidebilir, saklamanın da bir suç olduđu ařıkardır.

Bu bölümde web sitesi güvenliđi konusuna giriş yaptık. Ufak bir duyurumuz var. Ađ Güvenliđi Akademisi Güncesi (Blog) <http://agguvenligi.blogspot.com> adresinde yayına bařladı. Yazı dizisi hakkında özet bilgiler sunarak sizden yorumlarınızı toplamayı hedefliyoruz. Konuyla ilgili, Dilbert bařta olmak üzere çeřitli karikatürler de sitemizi řenlendirecek. Her türlü öneriniz için bana e-posta ile ulařabilirsiniz.