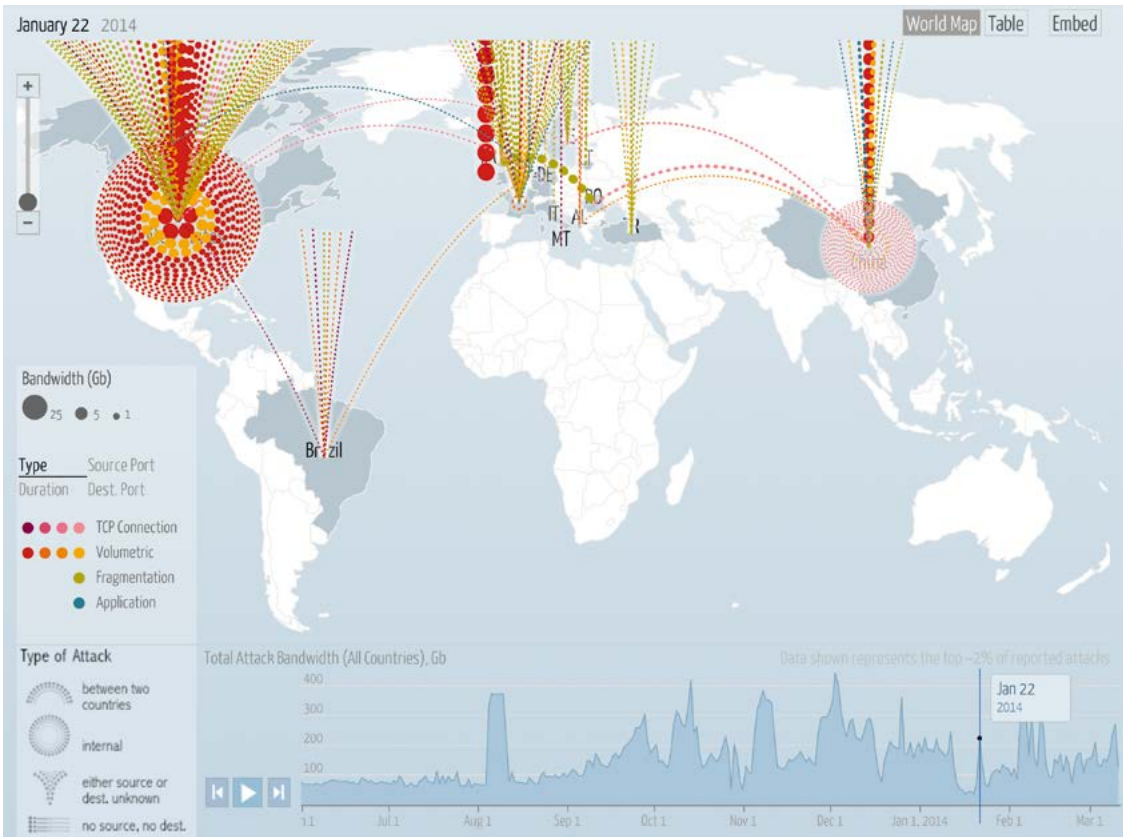
Börteçin Ege

DDoSSiber Saldırıları Önlenebilir mi?

DoS ve DDoS siber saldırılar son yıllarda bilgisayar korsanlarının en tercih ettiği saldırı yöntemlerinden biri. Peki, DoS veya DDoS saldırıların diğer siber saldırılardan ana farkı nedir, nasıl gerçekleştiriliyor, bunlardan etkili bir şekilde korunma yöntemleri var mı?



DoS saldırıları (*Denial of Service*) dendiğinde bir internet hizmetine erişimin engellenmesi anlaşılır. Bir DoS saldırısının birçok bilgisayar sistemi tarafından aynı anda ve ortaklaşa gerçekleştirilmesi durumunda ise bu teknik DDoS saldırısı (*Distributed Denial of Service*) olarak adlandırılır. Normalde bilgisayar korsanları tarafından düzenlenen saldırılar etkin olmaları açısından DDoS saldırıları olarak düzenlenir, fakat nadiren de olsa bir hizmete erişimin, sunucunun kendisindeki bir teknik problem veya kullanıcı kaynaklı, ani ve yoğun trafik üzerine de bir DoS veya DDoS saldırısına uğramadan engellenmesi veya sistemin çökmesi mümkündür.

Günlük yaşamdan bildiğimiz klasik siber saldırıların aksine DoS/DDoS saldırılarındaki asıl amaç bir bilgisayar sistemine sızmak değil, söz konusu sistemin sunduğu hizmetleri bloke etmektir. Bundan dolayı da saldırganların daha önceden herhangi bir şekilde temin edilmiş şifrelere ihtiyacı yoktur. DDoS saldırılarıyla ilgili akılda bulundurulması gereken diğer hususlardan biri de bu saldırıların bazı durumlarda amaç olmaması, aksine ilk anda akla gelenden daha farklı ve gizli bir hedefe hizmet eden araçlar olarak da kullanılabileceği gerçeğidir. Dolayısıyla bu tip siber saldırılar sistem yöneticilerinin karşısına dikkatleri dağıtmak için kullanılan, taktik bir yöntem olarak da çıkabilir. Kaliforniya'da 24 Aralık 2012'de,

yani geleneksel olarak Batı'da Noel döneminin doruk noktası olan günde bir bankaya başlatılan siber saldırıyla bilgi işlem personeli göstermelik bir DoS saldırısıyla meşgul edilirken, aynı sıralarda hem de hiç kimsenin ruhu duymadan aynı bankadaki bir hesabın ele geçirilerek söz konusu hesaptan neredeyse bir milyon dolar çalınması bunun tipik bir örneğidir.

DDoS saldırıları, daha önceden sızılan sistemlerde ele geçirilen bilgisayarlarda arka kapılar açılarak, bu bilgisayarların gelecekteki siber saldırılarda kullanılmaya hazır "zombi"ler haline dönüştürülüp zamanı geldiğinde etkinleştirilmesiyle gerçekleştiriliyor. Bu tip zombi bilgisayarlar topluluğu Botnet olarak da adlandırılıyor. Bu kapsamda az sayıda zombi bilgisayardan oluşan küçük Botnet'lerle bile çok etkili saldırılar düzenlenebildiği biliniyor. Nitekim, 2007'de Rusya merkezli gerçekleştirildiği iddia edilen tarihin ilk siber saldırılarından birinde, Avrupa'nın en gelişmiş bilgisayar ve internet sistemine sahip olan Estonya'da bankalara, devlet kurumlarına, radyo ve televizyon istasyonlarına ait internet sunucuları siber korsanlar tarafından birbiri ardına ele geçirilerek haftalarca kontrol altında tutulmuş ve bu saldırının koordine edildiği merkez hiçbir zaman tam anlamıyla tespit edilememişti. Bilinen tek gerçek üç milyonluk bir nüfusa sahip Estonya'nın "siber işgali" için sadece 50.000 zombi bilgisayardan oluşan bir Botnet'in fazlasıyla yeterli olduğuydu (bkz. Ege, B., "Siber Savaşlar: Bilişimin Karanlık Yüzü", *Bilim ve Teknik*, s. 18-22, Kasım 2012). Bir Botnet'in boyutu onlarca ve milyonlarca zombi bilgisayar arasında değişebiliyor. Bu zombi bilgisayarlar tarafından gerçekleştirilen siber saldırılardaki trafik yoğunluğu ise saniyede 350-400 Gbit gibi rekor seviyelere ulaşabiliyor ve genelde böyle durumlarda hedefteki sisteme teslim bayrağını çekmekten başka bir seçenek kalmıyor.

Her sistem durması DoS veya DDoSSaldırısı Anlamına Gelmiyor

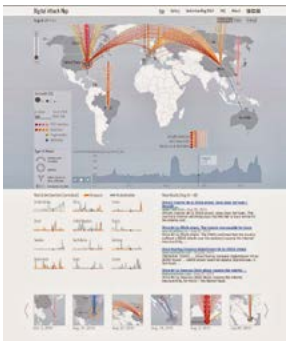
Yukarıda da kısaca değinildiği gibi bir sunucu tarafından verilen hizmete erişimin durması doğrudan o sistemin DoS veya DDoS gibi bir siber saldırıya maruz kaldığı anlamına gelmiyor. Herhangi bir teknik sorunun yanı sıra sisteme gönderilen karmaşık bir sorgu veya yine çok karmaşık bir hesap işlemi de söz konusu sistemin kısa veya uzun süreli olarak devre dışı kalmasına sebep olabiliyor. Fakat yine de, bir DDoS saldırısında olduğunun aksine, bu gibi teknik sorunların yaşanmasını önleyebilecek tedbirlerin alınması mümkün: Sunulan hizmetten aynı anda faydalanabilecek kullanıcı sayısının ve bu kullanıcıların her birine en fazla ne kadar teknik kaynak ayrılabileceğinin önceden belirlenmesi, ayrıca tüm hizmetlerin sadece tek bir IP adresi üzerinden değil de daha önceden tanımlanmış farklı faklı IP adresleri üzerinden verilmesiyle bu tip durumlardan kaçınılması ya da en azından bunların sayısının azaltılması mümkün.

Her Saniye Önemli

Tıpkı günlük hayatta olduğu gibi DoS ve DDoS saldırılarında da dikkat edilmesi gereken en önemli hususlardan biri söz konusu tehdit unsurlarının vakit kaybetmeden bir an önce deşifre edilmesidir, çünkü savunma mekanizmalarının etkili olarak çalışması ancak doğru zamanda devreye sokulmasıyla mümkündür. Burada göz önünde tutulması gereken diğer bir nokta da DoS ve DDoS saldırılarının her zaman aniden düzenlenen bir siber saldırı olmadığıdır. Geçmişte gözlemlenen bazı örnekler DoS ve DDoS saldırılarının karşı taraftaki altyapısının hazırlanmasının, hedef sisteme sezdirmeden haftalar, aylar hatta yıllar alabildiğini gösteriyor.

Sonuç

DoS ve DDoS saldırıları gelecekte de özellikle bilişim dünyasının başını ağrıtmaya devam edecek gibi görünüyor. İnternet ile birlikte fiziksel sınırların yavaş ama emin bir şekilde ortadan kalktığı günümüzde bir an önce bu alanda da uluslararası düzenlemelere gidilmesi ve olası riskleri en alt seviyeye çekmek için hassas bilişim süreçlerinin mümkün olduğunca çevrim dışı hale getirilmesi şart gibi görünüyor. Hatırlatılması gereken bir diğer husus da -kolaylıkla tahmin edilebileceği gibi- bu tip siber saldırıların etik olmamanın yanı sıra hukuksal açıdan da çok ciddi suç teşkil ettiği ve bu saldırıları düzenleyenlerin aldıkları hukuki risklerin farkında olması gerektiğidir.



Siber Saldırı Haritası

Google ve Arbor Networks tarafından hayata geçirilen Digital Attack Map (Siber Saldırı Haritası) adlı web sitesi küresel ölçekte an itibariyle gerçekleştirilen DDoS saldırılarını gösteriyor.

DDoS saldırılarıyla ilgili daha fazla bilgi almak ve sitenin arşivinde geriye dönük incelemelerde de bulunmak isteyen herkes siteyi ziyaret edebilir. Siteye digitalattackmap.com adresinden ulaşabilirsiniz.

Kaynaklar
- Maier, J., Tanger, V., "Maßnahmen gegen Distributed-Denial-of_Service-Attacken: Internet-Angriffe abwehren", *iX – Magazin Für Professionelle Informationstechnik*, Sayı 5, s. 40-48, Mayıs 2014.
- futurezone - Technology News, "Kaspersky: Gegen Cybersabotage machtlos", 9 Mart 2011. http://futurezone.at/digital-life/kaspersky-gegen-cybersabotage-machtlos/24.564.977