14/12/2015 Tarihinde Başlayan

DDoS Saldırısı

Kamuoyu Duyurusu

Nic.TR, ODTÜ, 21/12/2015

14/12/2015 tarihinde başlayan ve azalarak sürmekte olan Dağıtık Servis Kesintisi Saldırısı (DDoS) saldırısına ilişkin gelişmeler ve potansiyel sorular için yanıt teşkil edebilecek saptamalar aşağıda maddeler halinde özetlenmektedir.

a. 14 Aralık 2015 Pazartesi günü, yurtiçi ve dışında 5 (beş) ayrı noktada konuşlanmış bulunan 6 (altı) adet ".tr" alan adı sunucusuna doğru gelen DDoS saldırısına bağlı olarak çok ciddi ölçüde Internet bant genişliği yoğunlukları yaşanmıştır. Saldırı temel olarak, "DNS yükseltme saldırısı" (DNS Amplification Attack) olarak başlamıştır. Bu saldırı, ".tr" Alan Adları'ndan ilgili IP adreslerine ulaşılmasını engellemek amacıyla, sahte ağ trafiği üretmek de dahil olmak üzere, DNS sunucularımıza doğru yoğun ağ trafiği yollanması şeklinde ülke dışındaki kaynaklar tarafından organize bir şekilde gerçekleştirilmiştir.

b. İlerleyen saatlerde saldırı, sunucuların bulunduğu ağları işleten Telekom operatörlerinin yurtdışı bağlantılarını dolduracak (ve taşacak) seviyelere ulaşmıştır. Telekom operatörlerimiz bir üst ağ sağlayıcıları tarafında, filtre ve saldırı önleme tedbirleri alınma yoluna başvurmuşlardır. Bu durum bu tür saldırılarda uygulanan rutin bir yöntemdir.

c. Üst (upstream) Telekom operatörlerinde konuşlanmış birden fazla 40 Gbps kapasiteli iletişim hattında taşmalara yol açan, bazılarında zaman zaman 200+ Gbps yoğunluklarına erişen bant genişliği saldırıları gözlenmiştir. Bu toplu saldırının, bugüne değin dünya üzerinde yaşanmış en yoğun saldırılardan biri olduğu bilinmektedir.

d. Yurtdışında DNS sunucusunun bulunduğu Avrupa'nın Internet Örgütlerinden biri olan RIPE, ilgili trafiğin yoğunluğu nedeniyle DNS sunucumuzu kapatmak zorunda kaldığını ifade etmiştir. Bu zaman diliminde Nic.TR diğer 5 sunucusu ile saldırı karşısında çalışır durumdaki konumunu korumuştur.

e. Bu durum, ".tr" DNS sunucularına öncelikle geliş yönünde gecikmelere neden olmuştur. ".tr" DNS sunucularına erişildiği durumlarda ise DNS sunucularının verdiği yanıtların isteği yapan noktalara gidişi yönünde de gecikmelere neden olmuştur. Diğer bir deyişle, saldırganlar tarafından ana iletişim arterlerinde oluşturulmuş yapay ve yoğun trafik, ülke ağının önemli arterlerinde bazı tıkanmalara ve yavaşlamalara neden olmuştur.

f. Saldırının başladığı ilk anlardan itibaren gözlenen ve algılanan saldırgan stratejisi; (i) "yapılabilirse DNS sunucuları durdur ve ülkeyi karanlığa sürükle", (ii) "olmazsa, ağın daha derinliklerinde problem yarat ve başka hedef ara" şeklindedir. Bu bağlamda, saldırganlar (i) maddesinde sözü edilen hedeflerine ilk 36 saat içinde ulaşamamış ve ilerleyen günlerde (ii). madde ve diğer şekillerde saldırmaya devam etmişlerdir.

g. Ana arterlerdeki trafik yoğunluğu sırasında DNS sunucuların yanıt üretme performansında bir yavaşlık gözlenmemiştir. Bu saldırı şartları altında dahi, DNS sunucuların yükünün çok düşük seviyelerde seyrettiği, herhangi bir donanım ya da yazılım bazında yetersizlik içerisinde olunmadığı görülmektedir.

h. Trafik yoğunluğu, ülke içinde verilen çeşitli Internet servislerinde (e-posta alışverişinde bir miktar yavaşlık, web sitesinin bir miktar gecikme ile açılması, vb.) hız düşüklüğü şeklinde ortaya çıkan bazı olumsuzluklara sebep olsa da, ekibimizin ve koordinasyon içinde çalıştığımız Telekom operatörlerinin yoğun çabalarıyla ülke çapında çok önemli boyutlarda bir servis yavaşlığı gözlenmemiştir.

i. Yaşanan yavaşlığın Türkiye İnternetine etkisi homojen olmamıştır. Bazı arterlerde bir miktar yavaşlık yaşanırken, bazı diğer ağ parçalarında olağan hızın devam ettiği gözlenmiştir. Örnek olarak, Twitter, Facebook vb. sosyal ortamlar ve internet bankacılığı ortamları incelendiğinde yoğun bir şikayetin olmadığı, tersine bu ortamların problemsiz bir şekilde kullanıldığı görülmektedir.

j. Bu saldırının kaç kişi ve/veya kurumu etkilediği şeklinde bir soruya kolayca bir yanıt verilemez. Tek söylenebilecek olan, göreli bir yavaşlığın olduğu, ancak bunun günlük Internet yaşamını ve herkesi etkilemediğidir.

k. Eldeki verilerle saldırının kamu ve/veya özel sektör odaklı olup olmadığını ayıracak bir veri bulunmamaktadır. Ana arterlerden gelen trafik yoğunluğu nedeniyle her kesimin bir miktar yavaşlık şeklinde etkilenmiş olduğu söylenebilir.

l. Saldırı, sahte ağ trafiği üreterek ülke dışındaki kaynaklar tarafından gerçekleştirildiği için, bu tip saldırıların tek çözümü saldırı oluştuğunda ülkenin İnternet girişinin ana kapıları ve arterlerinde korunma sağlamaktır. Bu sözü edilen korunma biçimi ve önlemleri şu anda sürmektedir ve saldırının ileride tekrarlanması halinde de bu önlemlerin Telekom operatörlerimizce alınacağı açıktır.

m. Bu aşamada 3'ü yurt dışına olmak üzere toplam 11 alan adı sunucusu ile hizmet verilmektedir. Yurtdışındaki sunucularda uygulanan ANYCAST adlı teknik nedeniyle 11 sunucu pratikte 20'den fazla sunucu olarak hizmet sağlamaktadır.