DDoS Olay İnceleme ve Müdahale Raporu

SYN Flood Tabanlı Olağanüstü Boyutta DDoS Saldırısı

1. Özet

Network altyapımız 24 Kasım akşamı itibarıyla olağanüstü hacimde bir SYN Flood tabanlı Dağıtık Hizmet Engelleme (DDoS) saldırısına maruz kalmıştır. Bu saldırı yöntemi, TCP bağlantı kurulumu sırasında sunucuların yarım bıraktığı bağlantı isteklerini kötüye kullanarak oturum tablolarının dolmasına, CPU/Memory kullanımının aniden yükselmesine ve servislerin zaman zaman erişilemez hale gelmesine neden olmuştur.

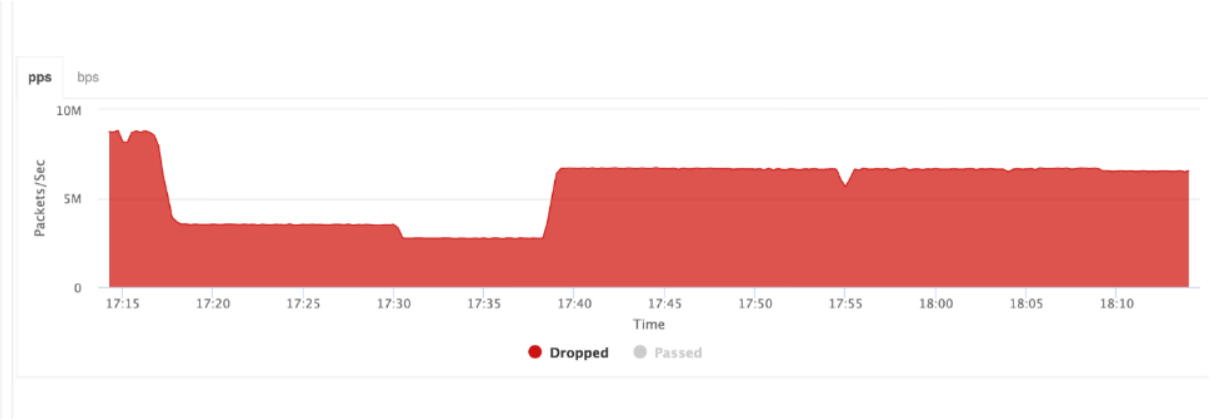
Saldırı süreci boyunca ISP ve datacenter hizmeti sağlayıcımız ile birlikte altyapıdaki koruma katmanları hem de global bağlantı sağlayıcıların sunduğu gelişmiş koruma mekanizmaları devreye alınmıştır. Alınan mitigasyon önlemleri ile birlikte zararlı trafik kademeli olarak kontrol altına alınmış, hizmet sürekliliği yeniden sağlanmıştır.

2. DDoS Etkileri ve Saldırı Boyutu

Gerçekleşen SYN Flood saldırısı, standart koruma mekanizmalarının öngördüğü kapasitenin üzerinde gerçekleşmiş olup birçok bileşeni aynı anda zorlamıştır.

Saldırı Trafiği

- Saldırı yoğunluğu: **6.5M – 10M PPS (packet-per-second)**
    - **((Global Ölçekte günlük gerçekleşen saldırı ortalaması 2.2M PPS)**
- Engellenen toplam trafik hacmi: **30 Terabayt**
    - **(Global Ölçekte günlük gerçekleşen saldırı ortalaması 3 Terabayt)**
- Kaynak IP çeşitliliği: Yüksek derecede dağıtık ve spoofed trafik



Etkiler

• Servislerimize erişimde belirli aralıklarda erişim kesintileri yaşanmıştır.
• Güvenlik cihazlarında CPU ve bellek kullanımında olağan dışı artış gerçekleşmiştir.
• Network portlarında saturasyon ve anlık trafik şişmeleri gerçekleşmiştir.
• Müşteri servislerinde gecikme, bağlantı reddi ve erişim esnasında paket kayıpları oluşmuştur.
• DDoS koruma cihazlarında limit aşımları yaşanmıştır.

3. Teknik İnceleme

Saldırının Karakteristiği

Saldırı, klasik SYN Flood yönteminin, yüksek PPS hacmiyle güçlendirilmiş varyantı şeklindedir. Amaç, TCP üçlü el sıkışma sürecini tamamlamadan (half open) connection tablosunu şişirerek servislerin yeni bağlantı kabul etmesini engellemektir.

Öne çıkan teknik bulgular:

- Yüksek miktarda sahte IP adreslerinden gelen SYN paketleri tespit edilmiştir.
- Aşağıdaki ekran görüntüsünde kırmızı ile işaretlenmiş ülkelerden olağanüstü seviyede eş zamanlı saldırılara maruz kaldık.
- Saldırı yoğunluğu sebebiyle ilk etapta firewall işlem sürelerinde (CPU-RAM) gecikmeler yaşanmıştır.

4. Olay Kronolojisi

Aşağıdaki zaman çizelgesi, saldırının başlangıcından mitigasyonun tamamlanmasına kadar geçen süreci kapsamaktadır.

- 24 Kasım Pazartesi 19.00

SYN Flood karakteristiğinde olağanüstü yoğunlukta trafik tespit edildi. İlk anomali alarmları tetiklendi, trafik beklenen paternlerin üzerine çıktı. ISP/DC hizmet sağlayıcımız tarafındaki DDoS koruma servisimiz saldırı başlangıcından itibaren devreye girmiştir. Zararlı trafikler servis sağlayıcı seviyesinde filtrelenmeye başlanmıştır.

- 25 Kasım Salı 01.00

DDoS cihazları üzerinde trafik analizinin ardından katman koruma profilleri sıkılaştırıldı. Aynı gün SYN Flood saldırıları yoğun şekilde devam etmiştir, global kaynaklı botnet hareketliliği artmıştır. Bu süre zarfında rate-limit, syn koruma yöntemleri ayrıca saldırgan IP adresler için sürekli olarak kara liste ve rate-limit uygulandı.
Ulusal siber olaylara müdahale merkezi (USOM) 'a da yaşanan saldırı ile ilgili bilgi verilip sistemleri üzerinden olay kaydı açılmıştır. Konu ile ilgili kendilerinin de bilgisi olduğu ve takip ettikleri bilgisi alınmıştır.

- 26 Kasım Çarşamba 04.00

Sistemlerin büyük kısmı koruma altına alınmıştır. Paket analizi, rate-limit ve signature tabanlı filtreler daha sıkı hale getirildi. Tüm bu önlemlere ek olarak global ölçekte koruma sağlayan L7 DDOS koruma çözümü aynı gün içerisinde hızlıca devreye alındı.
Bununla birlikte BTK ile görüşülmüş ve kendilerine süreç ile ilgili bilgi aktarımı sağlanmıştır.

- 26 Kasım Çarşamba 17.30

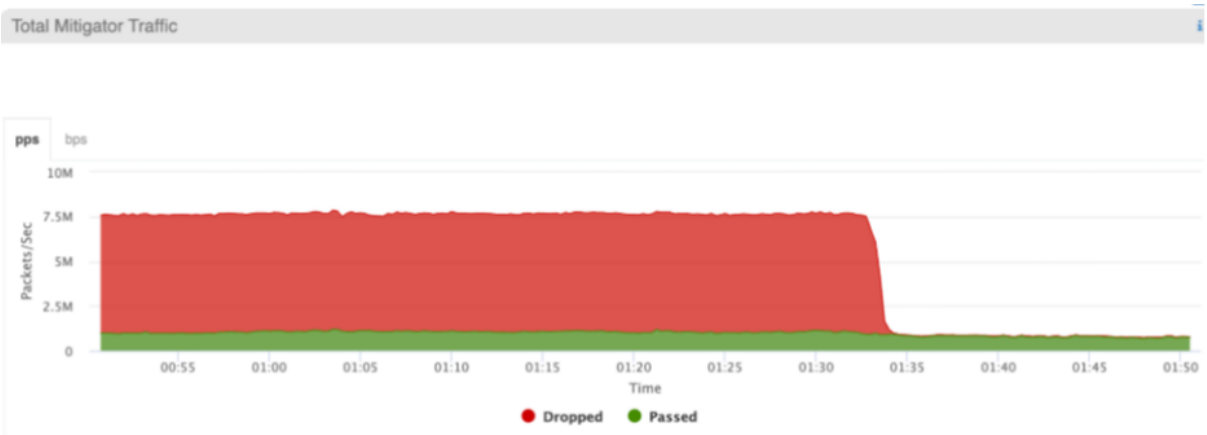
Kalan altyapı bileşenleri de ek koruma kapsamına alınarak tüm sistemler güvenli hale getirilmiştir. Saldırganların bu süre zarfında DDoS saldırı yöntemlerinde değişiklikler yaptığını tespit ettik. Bu nedenle saldırının karakteristik özelliğine uygun yeni profiler tanımlandı ve yeni gelen saldırılar başarıyla savuşturuldu. Eş zamanlı olarak koruma politikaları, müşteri hizmetlerinde minimum kesinti sağlanacak şekilde ileri seviye sıkılaştırma ile güncellendi. PPS limitleri optimize edildi, SYN koruma mekanizmaları agresif moda alındı.

- 27 Kasım Perşembe 18.00

Bu süreçte saldırı detaylarını gözlemlemeye ve sistemlerimiz üzerinde ek koruyucu önlemlerimizi almaya devam ettik. 18.00 itibariyle saldırı boyutu artış göstermiştir, sabah 01.35'e kadar devam etmiştir.

- 28 Kasım Cuma 01.35
-

Saldırıların saat 01.35 itibarıyla azaldığı gözlemlenmiştir.



5. Alınan Mitigasyon Önlemleri

Aşağıdaki çok katmanlı koruma adımları uygulanmıştır:

Network ve Güvenlik Katmanı

- SYN koruma mekanizmasının etkinleştirilmesi sağlanmıştır.
- Firewall üzerinde session limitlerinin sıkılaştırılması yapılmıştır.
- Rate-limit, connection-limit ve anomaly-based kuralların güncellenmesi gerçekleştirilmiştir.
- TCP timeout değerlerinin optimizasyonu sağlanmıştır.
- IPS/DoS politikalarının yeniden düzenlenmesi sağlanmıştır.

Altyapı İyileştirmeleri

- Ani yoğunlukları absorbe edecek şekilde bant genişliği 2 katına çıkartılmıştır.

6. Süreç Sonrası Değerlendirme

Saldırının hacmi ve süresi dikkate alındığında, gerçekleştirilen DDoS girişimi olağanüstü yoğunlukta olup küresel ölçekte organize botnet modelleri ile uyumludur. Alınan mitigasyon adımları sayesinde:

- Servis kesintileri minimize edilmiş,
- DDoS trafiği kontrollü şekilde filtrelenmiş,
- Hizmet altyapısı stabil hale getirilmiştir.

Genel değerlendirmede, mevcut DDoS koruma seviyesinin bu tür büyük ölçekli saldırıları karşılayabilmesi önemli bir kazanım olarak not edilmiştir. Saldırı süreci, proaktif izleme ve hızlı müdahale ile başarıyla yönetilmiştir.