DDOS ATTACK

(DAĞITIK HİZMET ENGELLEME)

DDOS ATTACK NEDİR ?

- Bir sistemi belirli kapasite sınırlarının üstünde veriye maruz tutma yoluyla düzenlenen saldırılar sonucu kullanıcıların **sisteme veya siteye girişinin engellenmesidir.**

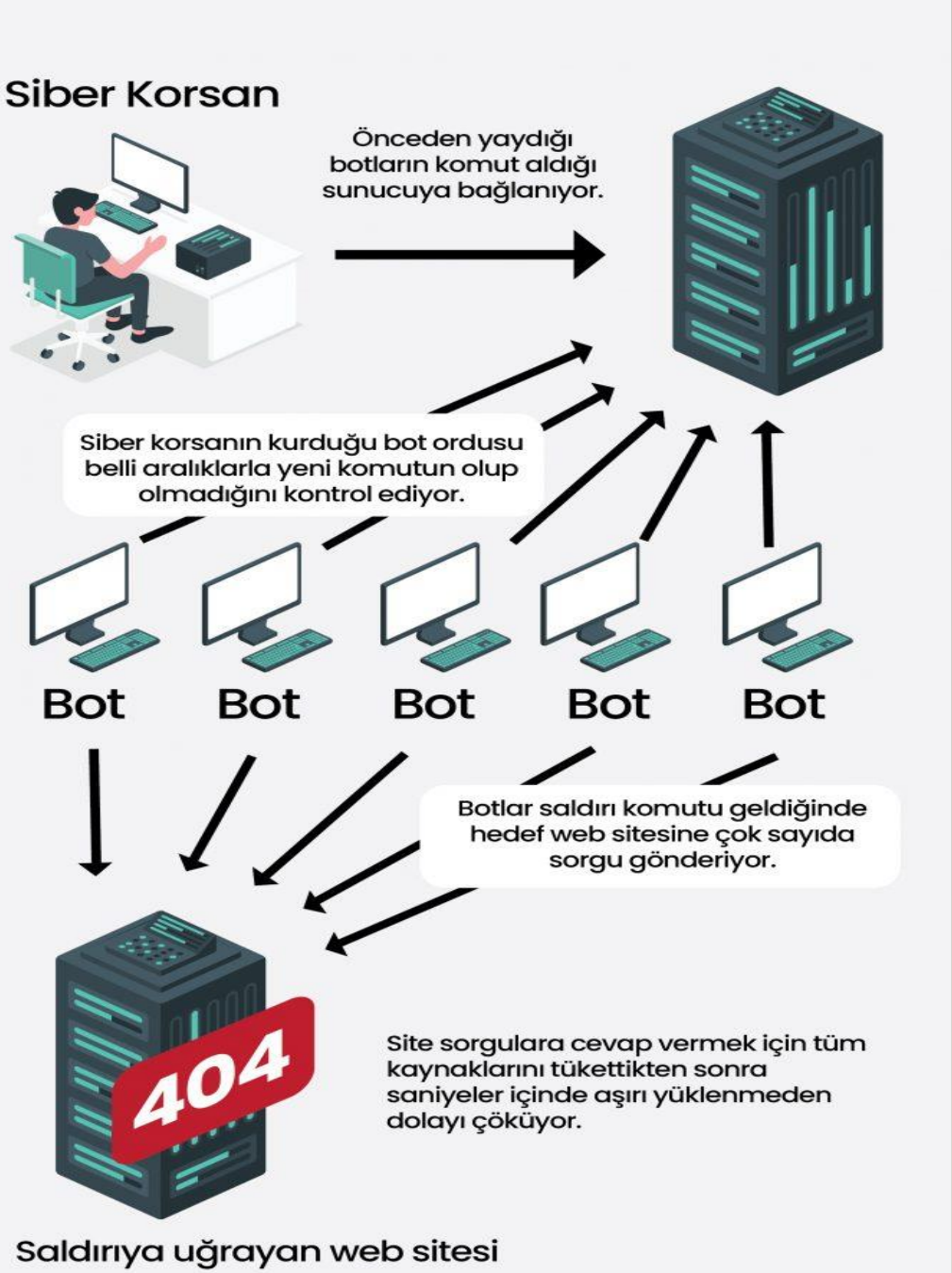
AMACI

- Sunucunun ya da ağın kaldıramayacağı kadar trafik oluşturarak çalışamaz / erişilemez hale getirmek.
- Sisteme ve siteye girişi engelleme.
- Amaç tamamen hedefi kullanılamaz duruma getirmek ve hizmeti engellemektir.

DDOS SALDIRILARI NASIL YAPILIYOR?

- DDoS saldırıları, internete bağlı cihaz ağları ile gerçekleştirilir. Bu ağlar, her birine bot (zombi) denen kötü amaçlı yazılım bulaşmış ve bir saldırgan tarafından uzaktan kontrol edilen cihazlardan oluşur. Saldırganlar, botnet oluşturmak için güvenlik açıklarından yararlanarak, cihaz sahiplerinin bilgisi olmaksızın cihazlara kötü amaçlı yazılım enjekte ederler. Bir botnet'te (botlardan oluşan ağ) uzaktan kontrol edilen binlerce veya milyonlarca cihaz olabilir.

- Bir botnet kurulduktan sonra artık saldırgan her bir bota uzaktan talimat göndererek saldırıya yönlendirebilir. Bir sunucu veya ağ botnet tarafından hedeflendiğinde, her bot hedefin IP adresine istekler gönderir ve potansiyel olarak sunucunun veya ağın aşırı yüklenmesine neden olur. Böylece sunucu veya ağ normal trafiğe hizmet edemez hale gelir.



DDOS SALDIRLARININ BELİRTİLERİ

- Ağır çalışan ya da hiç çalışmayan web siteleri DDoS saldırısının nedeni olabilir. Aşırı network kullanımı ise DDoS saldırılarının en büyük belirtisidir. Bunların yanı sıra yine aşırı UDP, SYN ve GET/POST sorguları da genellikle DDoS saldırılarının belirtileri arasında gösterilebilir.

SLOWLORİS NEDİR ?

- Slowloris , tek bir makinenin başka bir makinenin web sunucusunu minimum bant genişliği ve alakasız hizmetler ve bağlantı noktaları üzerinde yan etkilerle kapatmasına izin veren bir tür hizmet reddi saldırı aracıdır.
- Amaç, hedef web sunucusuna birçok bağlantıyı açık tutmaya ve bunları mümkün olduğunca uzun süre açık tutmaya çalışır.

DDOS SALDIRISI NASIL ÖNLENİR?

- Ne yazık ki, DDoS saldırılarının hedefi olmaktan korunmanın kesin ve kalıcı bir çözüm yolu yoktur. Ancak hedef olma ihtimalini ve saldırı etkilerinin azaltılmasını sağlayabilecek bazı yöntemler bulunmaktadır.
- Erken önlem almanız en iyi savunma yollarından birisi olduğu için oldukça önemlidir. Ancak bu belirtileri sisteminizde yaşanan anlık ve normal performans artış / azalışlarından ayırmak doğru teknoloji ve uzmanlık gerektirmektedir.
- İşletmeler açısından ise öncelikle çalışılan network altyapısının iyi tasarlanmış olması ve ilgili personelin sistem ve TCP/IP bilgisinin üst düzey olması korunma önlemlerinin başında gelmektedir.
- Bunun haricinde gerçekleştirilecek bazı uygulamalar ile DDoS saldırılarından korunmak ya da saldırı etkisini azaltmak mümkündür.

DDOS SALDIRISI BİLGİ GÜVENLİĞİN HANGİ UNSURUDUR ?

DDOS saldırısı bilgi güvenliğinin ‘ Erişebilirlik ’ bileşenini hedef alır. Çünkü DDOS saldırıları birden fazla kişinin aynı anda giriyormuş gibi yapıp sistemi yanıt vermez hale getirir. Sisteme olan erişebilirliğini kısıtlar.

Gizlilik olmaz çünkü erişim yetkisi olan kişilerin girişiyle ilgili bir durum söz konusu değildir.

Bütünlük olmaz çünkü bilgi işleme yöntemlerinin doğruluğu ve bütünlüğünü etkileyen bir durum söz konusu değildir.