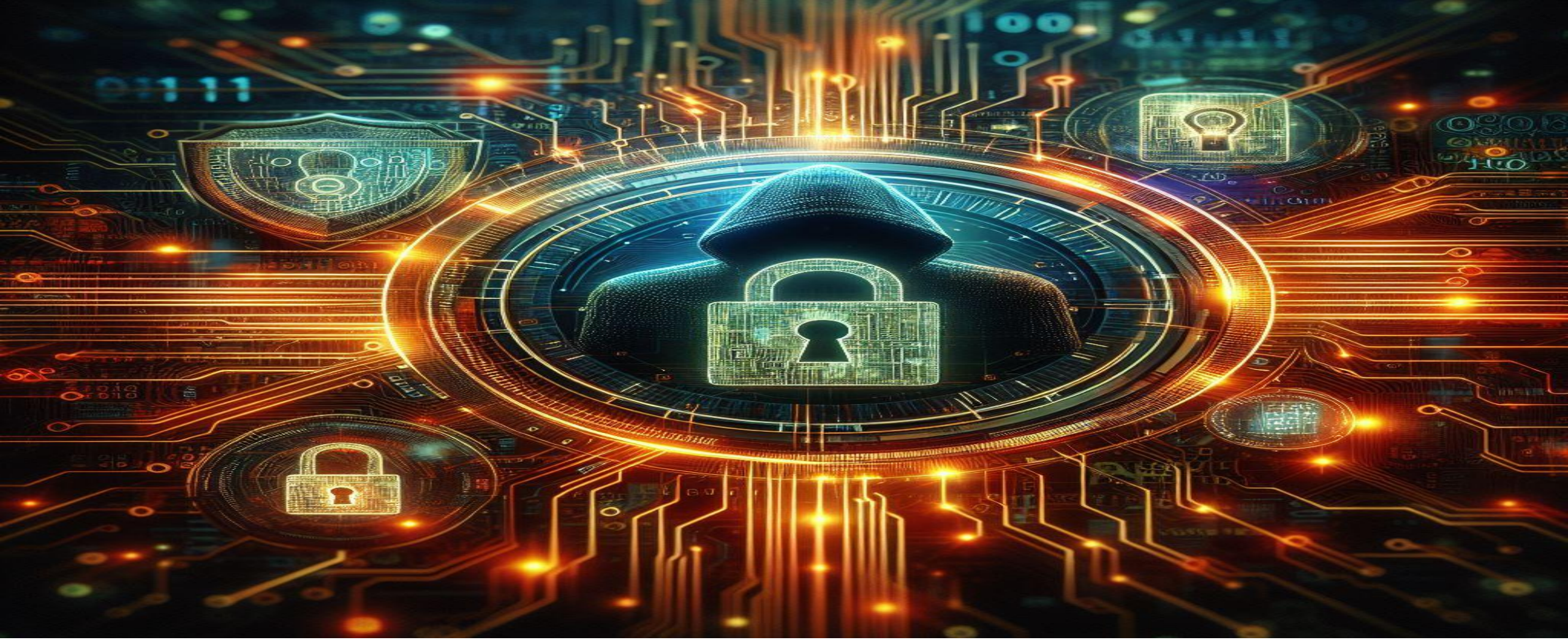


NETWORK SECURITY

Lecturer Erhan AKAGÜNDÜZ

ATTACK METHODS

- ✓ Saldırılar ağ üzerinden olacağından ağa bağlı cihazlar her zaman saldırıya açık durumdadır durumdadır.
- ✓ Saldırganlar ağ üzeriden hedef makinaya ulaşarak yazılım veya donanıma zarar vermek isteyebilir.
- ✓ Bunun yanı sıra bir işletmenin ağına ulaşarak veritabanındaki verilere erişebilir, değiştirebilir veya silebilir.

ATTACK METHODS

- ✓ Saldırgan ağın İnternet bağlantısını kesebilir.
- ✓ Hedef makinaya truva atı gibi program yükleyerek kullanıcıyı takibe alabilir.
- ✓ Aynı zamanda saldırgan ağa girebilmek için farklı yöntemler kullanabilir.

DENIAL OF SERVICE - DOS

- ✓ Hizmet reddi (Denial of service-DoS) hizmet aksatma amaçlı bir saldırı çeşitidir.
- ✓ Bir sisteme yapılan düzenli saldırılar sonucunda sistem çalışamaz ve hizmet veremez hâle gelebilir.
- ✓ Ayrıca DoS saldırılarıyla hedef sisteme ait kaynakların tüketilmesi de amaçlanır.

DENIAL OF SERVICE - DOS

- ✓ Bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hâle gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlanır.
- ✓ Bu saldırı önemli sunucuların servis vermeyi durdurması gibi büyük sorunlara yol açabilir.

DENIAL OF SERVICE - DOS

- ✓ Bir DoS saldırısının yaptıkları;
  - ❑ Network'ü trafik ile doldurmak böylece normal network trafiğini engellemek,
  - ❑ İki makine arasındaki iletişimi bozar, bu sayede bir servise erişimi engeller,
  - ❑ Özel birinin bir servise erişimini engeller,
  - ❑ Servisin belirli bir sistem veya kişi ile iletişimini bozar.

DENIAL OF SERVICE - DOS

- ✓ Günümüzde en çok karşılaşılan yaygın DoS saldırısı şunlardır:
- ✓ **SYN (eşzamanlı) taşması:** Sunucuya gönderilen ve istemci bağlantısı isteyen paket taşmasıdır. Paketlerde kaynak IP adresleri geçersizdir. Sunucu bu sahte isteklere yanıt vermekle uğraşırken geçerli isteklere yanıt veremez.

DENIAL OF SERVICE - DOS

- ✓ **Ping of death (Ölüm pingi):** Bir cihaza, IP tarafından izin verilen maksimum boyuttan (65,535 bayt) büyük bir paket gönderilir. Bu tür saldırılar artık bilgisayar sistemleri üzerinde etkili değildir.

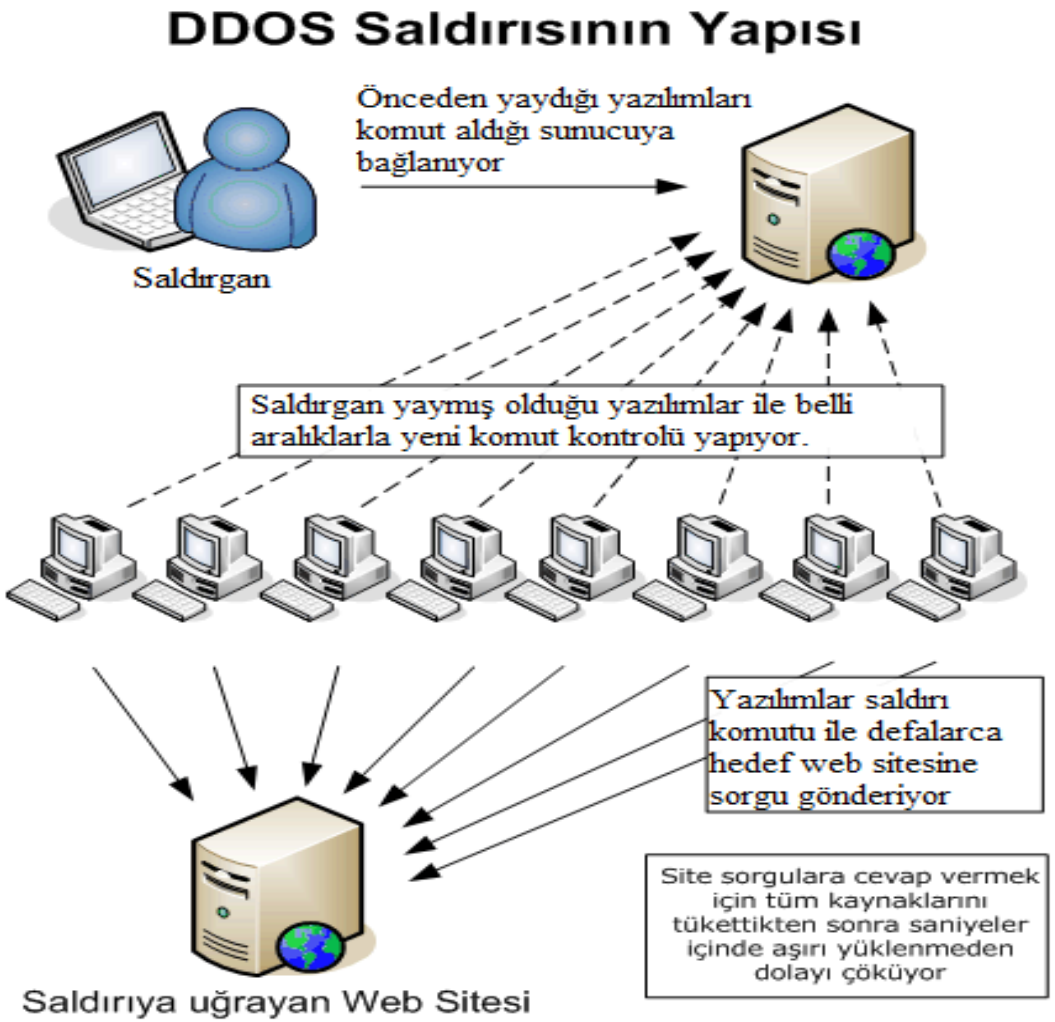
DISTRIBUTED DENIAL OF SERVICE–DDOS

- ✓ Dağıtılmış hizmet reddi (DDoS) saldırıları DoS saldırılarının farklı kaynaklardan yapılması ile gerçekleşir.
- ✓ Saldırganlar bazı yazılımlar tasarlayarak (Truva atı, solucan vb.) bu yazılımları
- ✓ İnternet kullanıcılarına e-mail ya da çeşitli yollarla yükleyerek geniş kitlelere yayar.

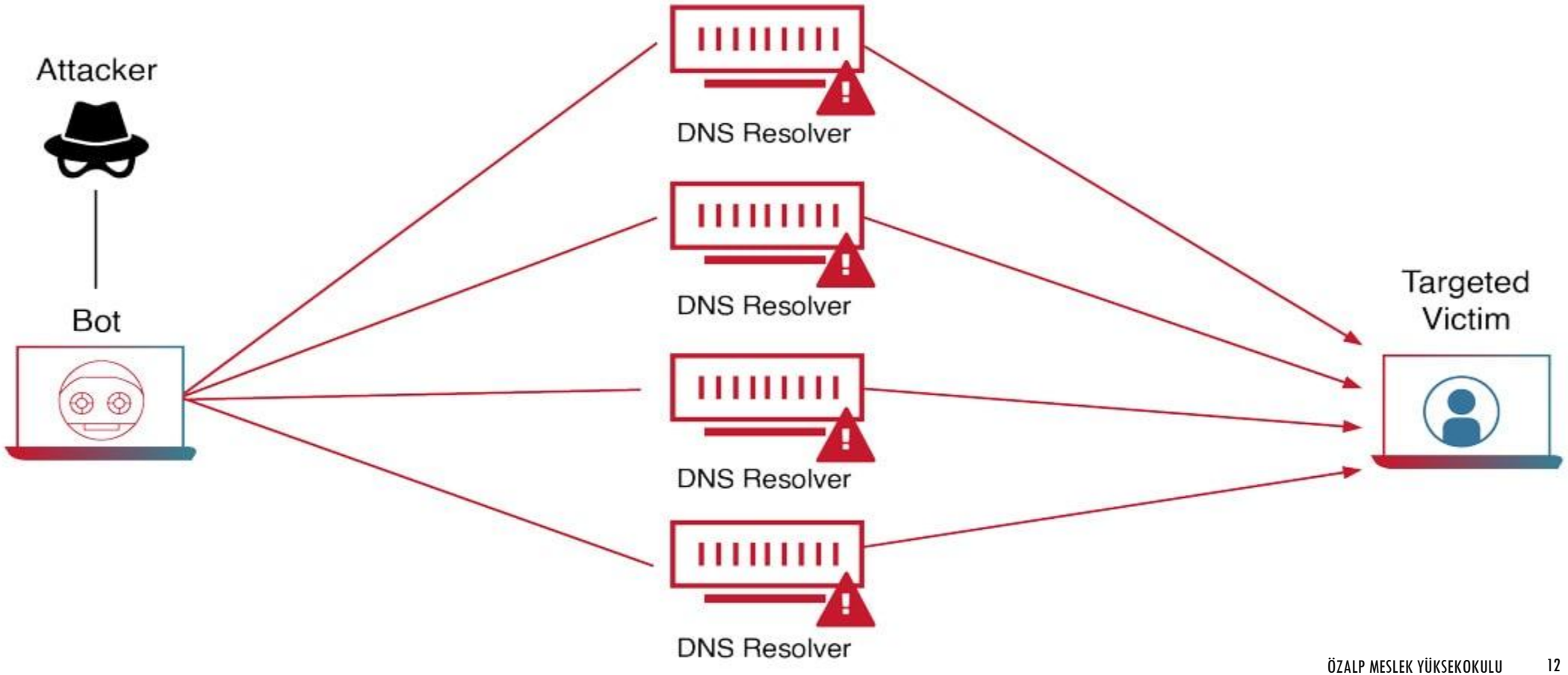
DISTRIBUTED DENIAL OF SERVICE–DDOS

- ✓ Bu şekilde yetki elde ettikleri çok sayıdaki İnternet kullanıcılarının bilgisayarlarını istedikleri zaman istedikleri siteye binlerce sorgu göndermek için kullanır.
- ✓ Saldırganın kontrolü altındaki onlarca bilgisayardan tek bir sunucuya binlerce sorgu göndermekte; bu da hedef makinenin band tüketmesine ya da tıkanmasına neden olmaktadır.

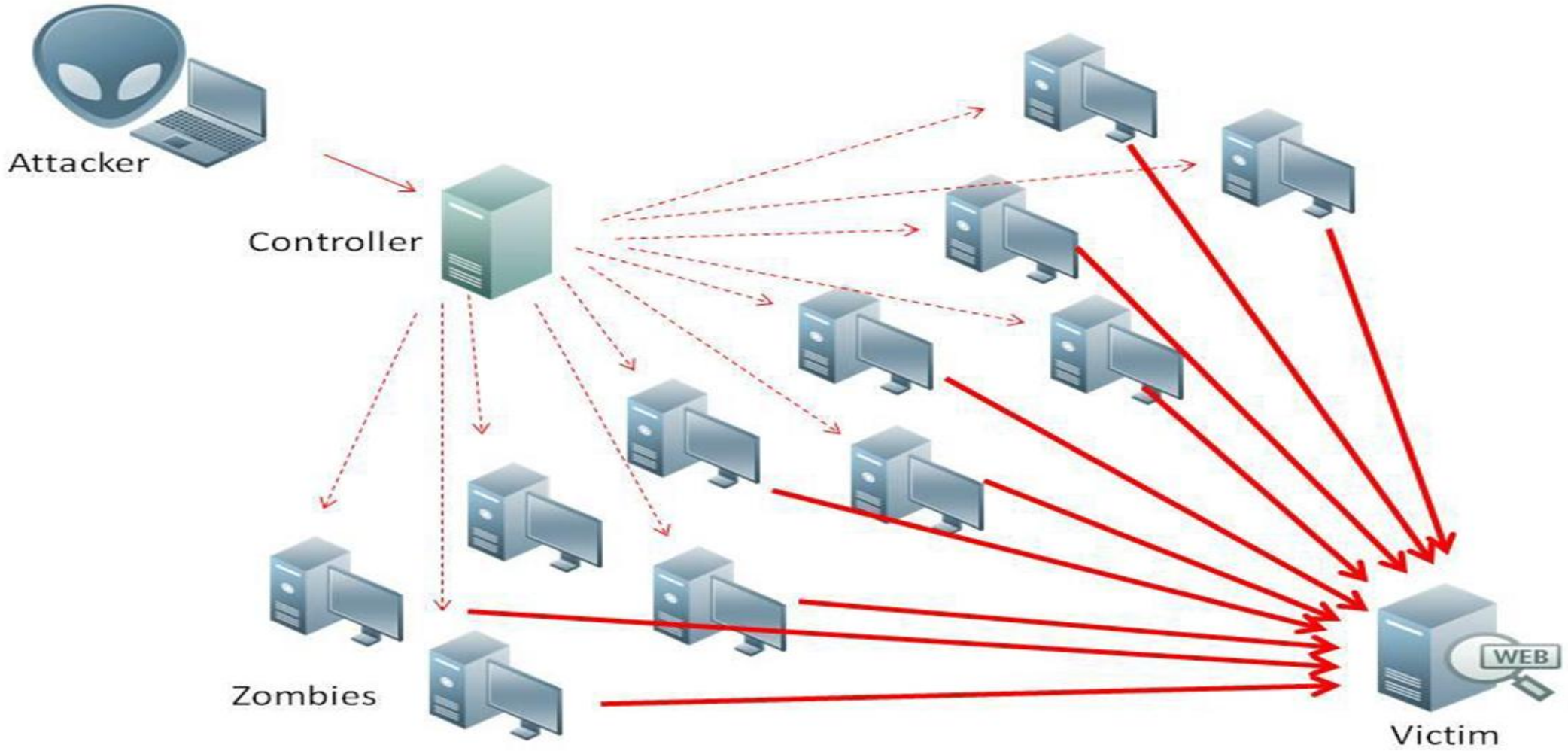
DISTRIBUTED DENIAL OF SERVICE–DDOS



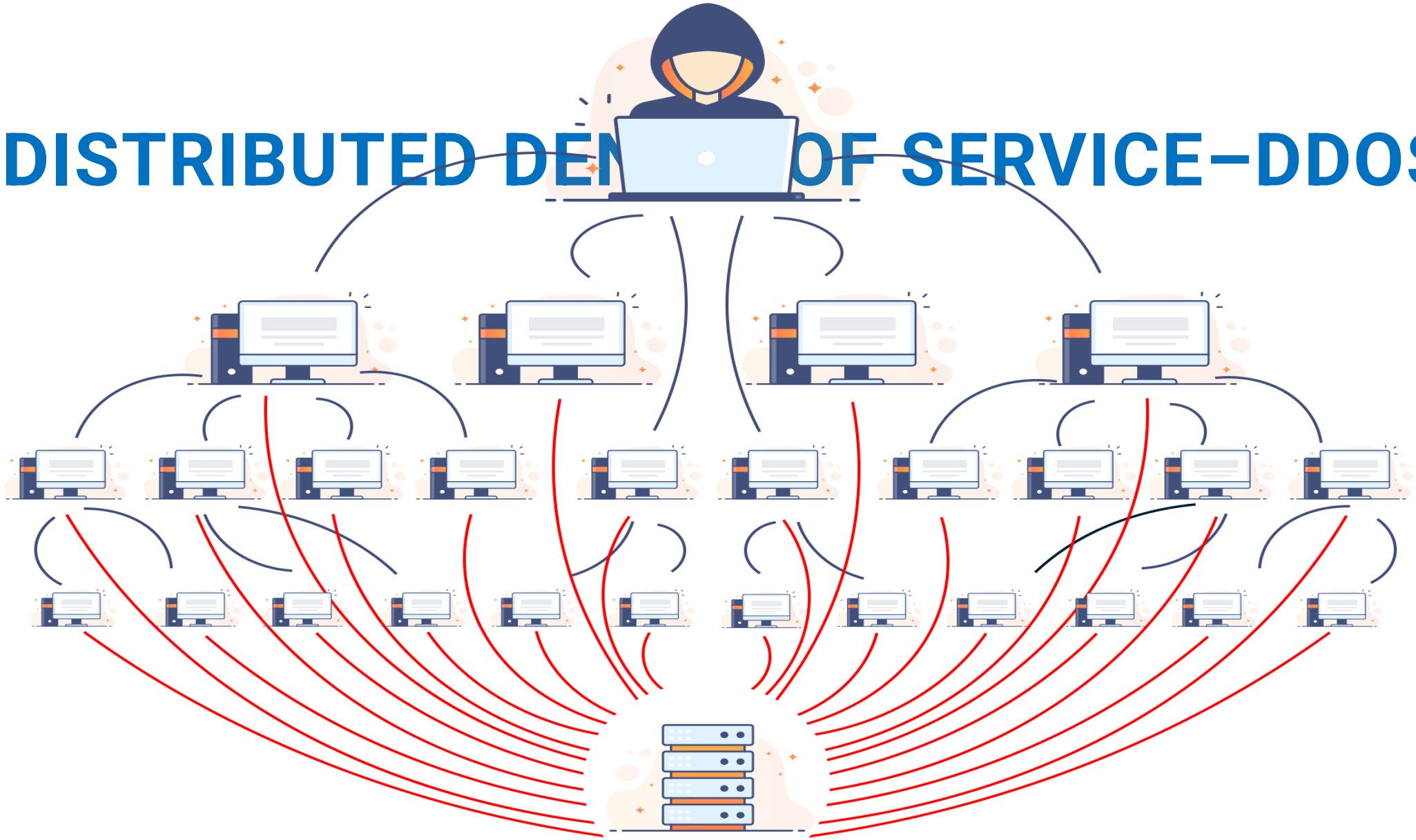
DISTRIBUTED DENIAL OF SERVICE–DDOS



DISTRIBUTED DENIAL OF SERVICE–DDOS



DISTRIBUTED DENIAL OF SERVICE–DDOS



DENEME YANILMA

- ✓ Ağ kesintilerine yol açan saldırıların tümü özel olarak DoS saldırıları değildir.
- ✓ Hizmet reddine yol açabilen başka bir saldırı türü de deneme-yanılma saldırısıdır.
- ✓ Deneme yanılma saldırılarında hızlı bir bilgisayar, parolaları tahmin etmeye veya bir şifreleme kodunun şifresini çözmeye çalışmak için kullanılır.

DENEME YANILMA

- ✓ Saldırgan, koda erişim kazanmak veya kodu çözmek için art arda hızlı şekilde çok sayıda olasılığı dener.
- ✓ Deneme yanılma saldırıları, belirli bir kaynakta aşırı trafik oluşması nedeniyle veya kullanıcı hesaplarının kilitlenmesiyle hizmet reddine yol açabilir.

SPYWARE

- ✓ Casus yazılım (spyware) kişisel bilgi toplama veya kullanıcının onayı alınmadan bilgisayarın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren programlardır.
- ✓ Casus yazılımlar genellikle kullanıcının onayı alınmadan bilgisayara kurulur.

SPYWARE

- ✓ Kurulduktan sonra kullanıcının internette gezinti bilgileri toplanabilir.
- ✓ Bu bilgiler reklam veren kişi ya da kuruluşlara veya İnternetteki diğer kişilere gönderilir ve parola, hesap numarası gibi bilgileri de içerebilir.

SPYWARE

- ✓ Casus yazılım genellikle bir dosya indirilirken, başka bir program yüklenirken veya bir açılır pencereye tıklandığında bilmeden yüklenir.
- ✓ Bilgisayarı yavaşlatabilir ve dâhili ayarları değiştirerek diğer tehditler için daha fazla zayıflık oluşturabilir.
- ✓ Ayrıca casus yazılımı bilgisayardan kaldırmak çok zor olabilir.

SPYWARE

- ✓ Casus yazılımlardan korunmak için;
- ✓ İşletim sisteminin güvenlik duvarı etkinleştirilmelidir.
- ✓ İşletim sistemi güncelleştirilmesi yapılmalıdır.
- ✓ Tarayıcının güvenlik ayarı yapılmalıdır.
- ✓ Anti-virüs yazılım kullanılmalıdır.
- ✓ İnternetten dosya yüklenirken dikkat edilmeli ve dosya antivirüs taramasından geçirilmelidir.

ADWARE

- ✓ Reklam yazılımı, kullanıcının ziyaret ettiği web siteleri temel alınarak kullanıcı hakkında bilgi toplamak için kullanılan yazılım biçimidir.
- ✓ Bilgiler daha sonra hedeflenmiş reklamcılık için kullanılır.
- ✓ Reklam yazılımı genellikle "**ücretsiz**" bir ürün karşılığında kullanıcı tarafından yüklenir..

ADWARE

- ✓ Kullanıcı bir tarayıcı penceresini açtığında, Reklam yazılımı kullanıcının İnternetteki sörf hareketlerine dayanarak ürün veya hizmetlerin reklamını yapan yeni tarayıcı pencerelerini açabilir.
- ✓ İstenmeyen tarayıcı pencereleri ard arda açılarak, özellikle internet bağlantısı yavaş olduğunda İnternette sörf hareketini çok zor hale getirebilir.
- ✓ Reklam yazılımının kaldırılması çok zor olabilir.

POP-UP

- ✓ Açılır pencereler bir web sitesi ziyaret edildiğinde görüntülenen ek reklam pencereleridir.
- ✓ Reklam yazılımından farklı olarak, açılır pencereler kullanıcı hakkında bilgi toplamak için tasarlanmamış olup genellikle yalnızca ziyaret edilen web sitesiyle ilişkilidir.
- ✓ Açılır pencereleri engellemek için tarayıcı özelliklerinden açılır pencere engelleyicisini etkinleştirmek gerekmektedir.

SPAM

- ✓ Bir e-postanın talepte bulunmamış, birçok kişiye birden, zorla gönderilmesi durumunda, bu e-postaya istenmeyen e- posta yani spam denir.
- ✓ Spamlar genellikle kitlesel veya ticari amaçlı olabilir.
- ✓ Satıcılar bazen hedeflenmiş pazarlamayla uğraşmak istemez.

SPAM

- ✓ Ürün veya hizmetlerinin birilerinin ilgisini çekmesi umuduyla e-posta reklamlarını olabildiğince fazla son kullanıcıya göndermek ister.
- ✓ Spam; İnternet hizmeti sağlayıcısını, e- posta sunucularını ve tek tek son kullanıcı sistemlerini aşırı yükleyebilen ciddi bir ağ tehdididir.

REFERENCES

Ağ Temelleri Ders Modülleri– MEGEP MEB (2011)