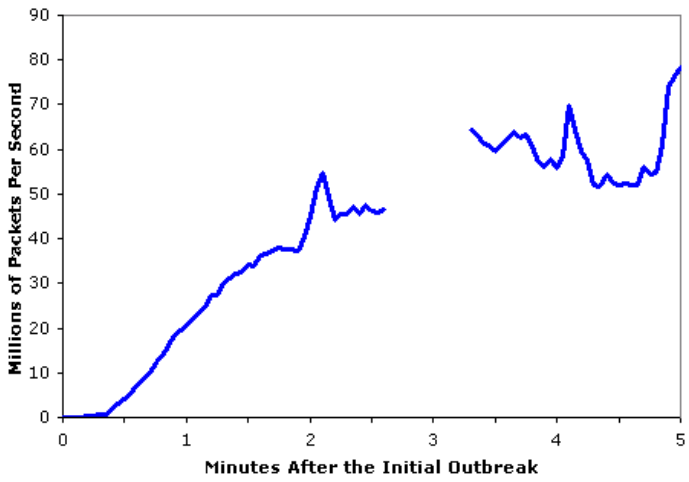
Ağ Güvenliği

- Internet altyapısına saldırılar:
  - Host'lara saldırılar: malware (kötü niyetli), spyware (casus), worms (solucanlar), yetkisiz erişim (veri çalma, kullanıcı hesapları)
  - Servis reddetme: kaynaklara erişimi reddetme (sunucular, linkin bant genişliği)
- Internet orjinalinde güvenlik tedbirleri düşünülerek oluşturulmadı
  - *orjinal görüş:* "birbirine güvenen insanlar bir ağa bağlanacak" ☺
  - Internet protokol tasarımcıları kötü niyetli irşimlere yetişip tedbir almaya çalışıyorlar
  - Bütün tabakalarda güvenlik düşünülüyor!

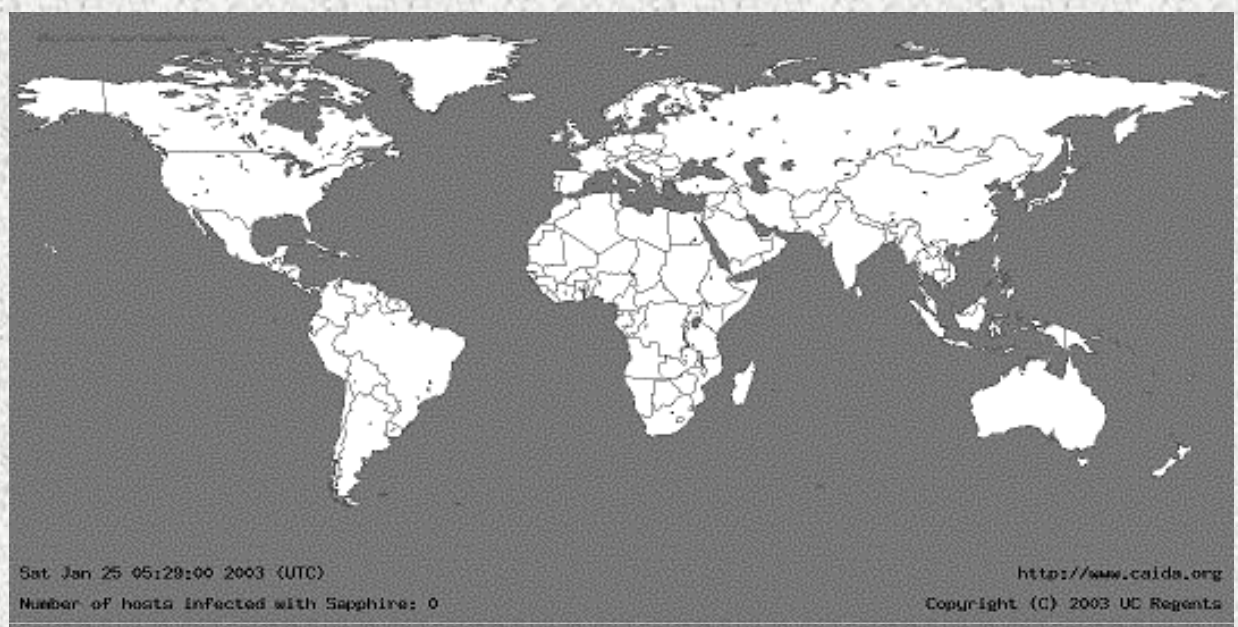
Kötü niyetliler ne yapabilir: malware?

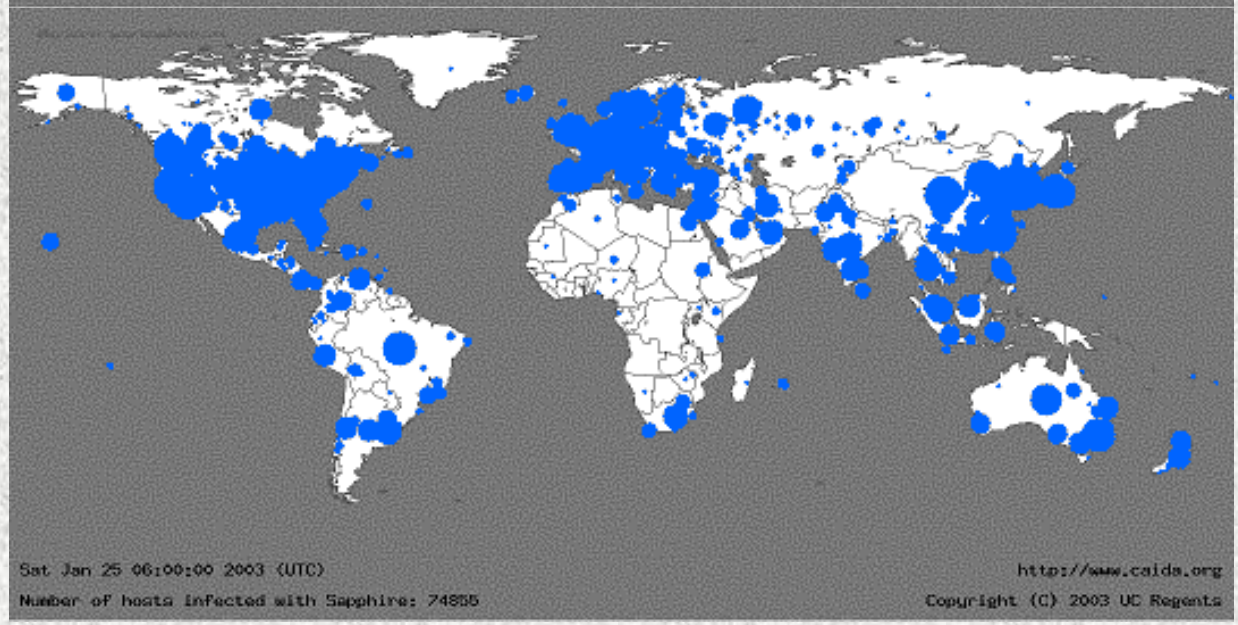
- Spyware (casus yazılım):
  - spyware olan bir web sayfasını indirerek bulaşır
  - Tuş vuruşlarını, ziyaret edilen web sitelerini kaydeder ve kötü niyetli kişiye gönderir
- Virus
  - Alınan bir yazılımın açılmasıyla bulaşır (e.g., e-mail eki),
  - Kendini çoğaltır: diğer kullanıcılara yayılır
- Worm (solucan):
  - Kendi kendini aktif hale getiren bir nesneye farkında olmadan alarak bulaşır
  - Kendini çoğaltır: diğer kullanıcılara yayılır

Sapphire Worm (2003): aggregate scans/sec in first 5 minutes of outbreak (CAIDA, UWisc data)



30 dakika sonra

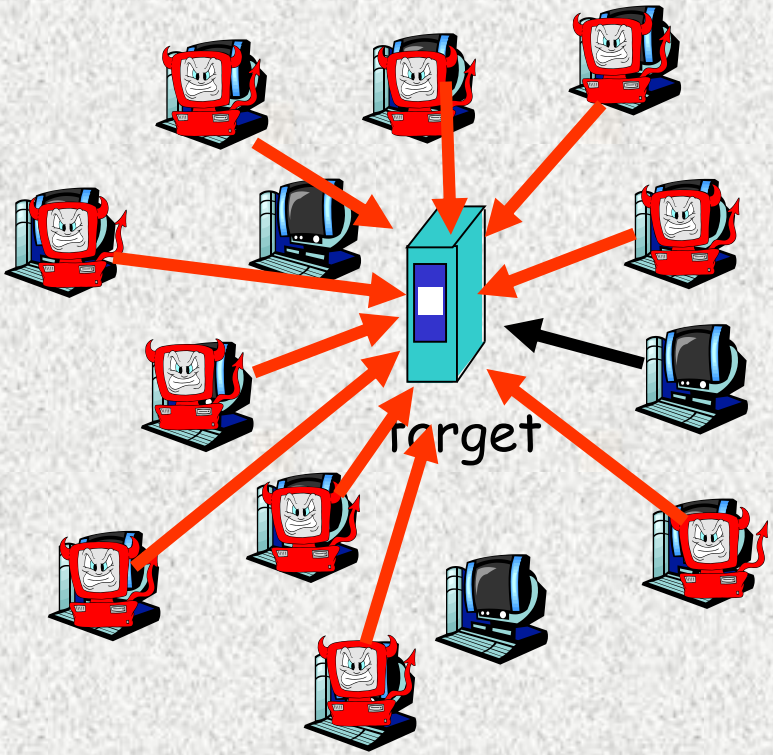




Servis reddetme saldırıları

- Saldırganlar sunucuya aşırı trafik yükleyerek servis vermesini engellerler

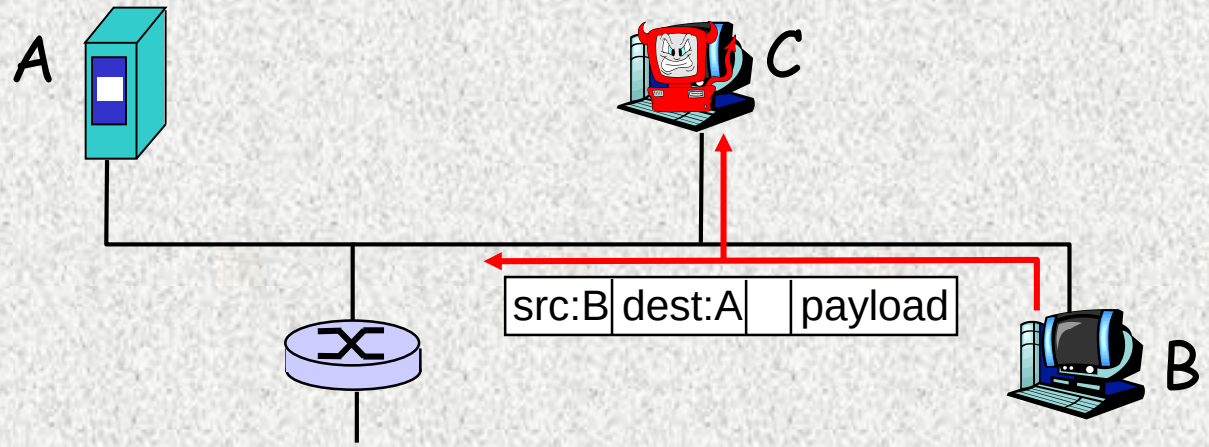
1. Hedefi seç
2. Ağdaki hostları kullan (bir malware yardımıyla)
3. Hedefe ele geçirilen hostlardan paket gönder



Paketleri kokla, değiştir, sil

Packet koklama:

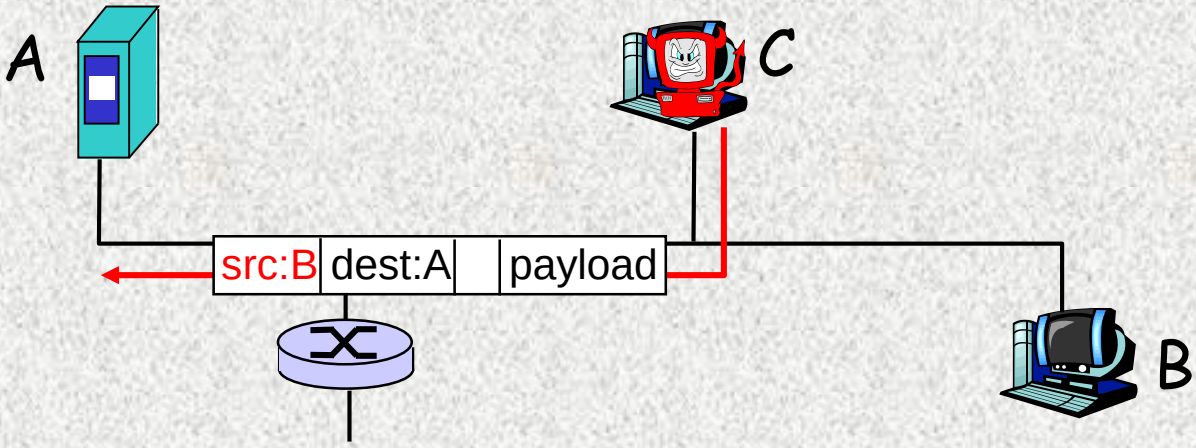
- broadcast ortamı (paylaşımlı Ethernet, kablosuz)
- Ortamdaki paketler okunur (e.g., şifrelerde tabii!)



- Daha sonra kullanacağımız Ethereal yazılımı bir paket koklayıcıdır
- Değiştirme ve silme konusu ileride

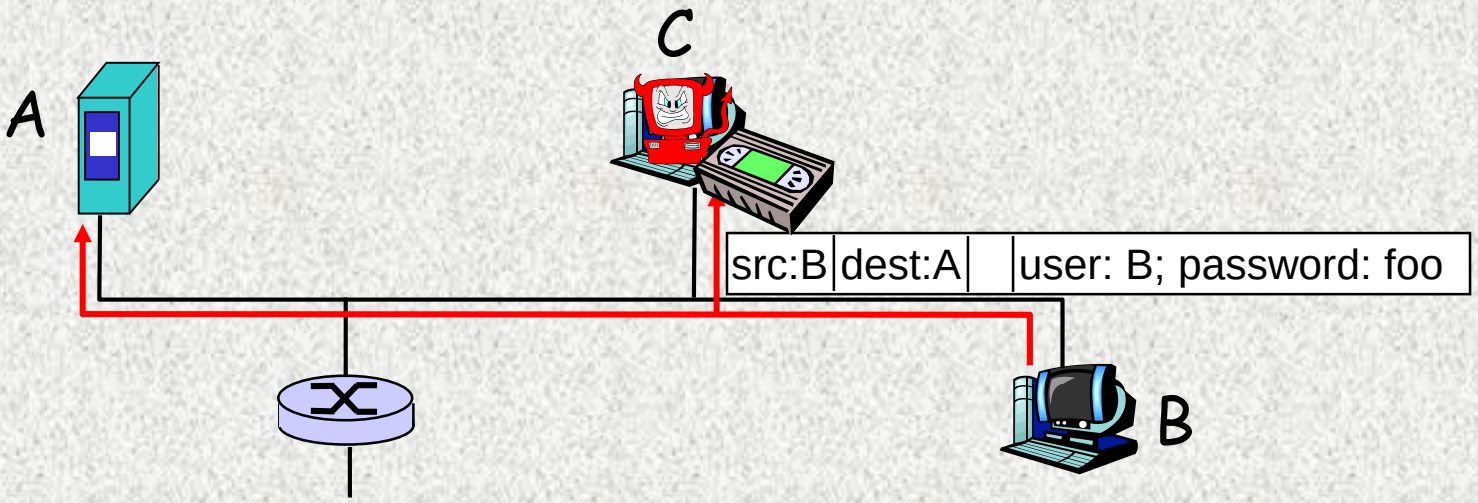
Sizin kılığınıza girme

- *IP spoofing:* Sahte kaynak adresiyle paket göndermek



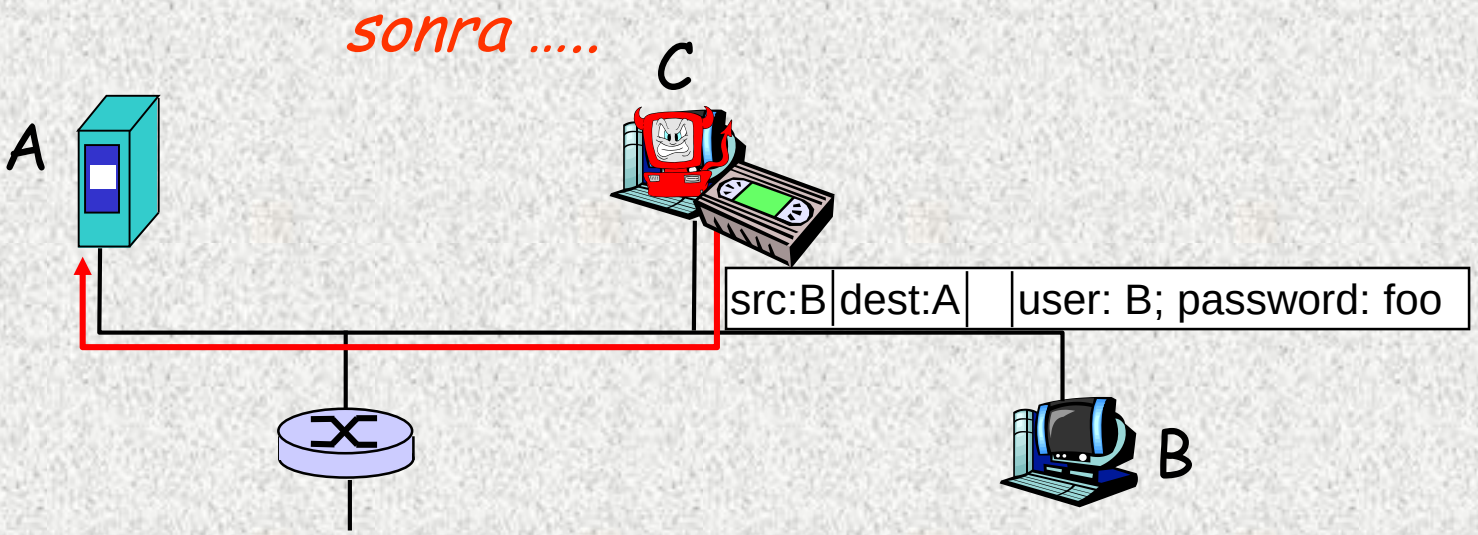
Sizin kılığınıza girme

- *IP spoofing:* Sahte kaynak adresiyle paket göndermek
- *Kaydet ve kullan*: önemli bilgileri kokla (e.g., şifre), ve sonra kullan



Sizin kılığınıza girme

- *IP spoofing:* Sahte kaynak adresiyle paket göndermek
- *Kaydet ve kullan*: önemli bilgileri kokla (e.g., şifre), ve sonra kullan



Ağ güvenliği

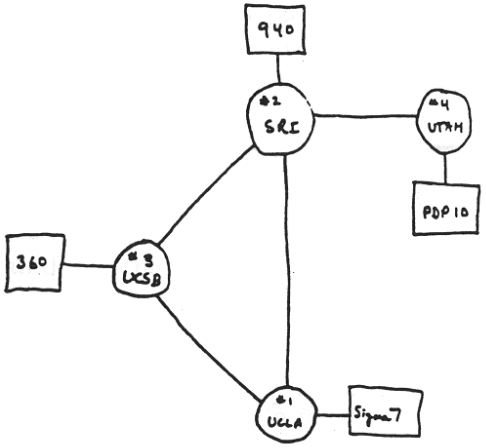
- İleride değineceğiz
- şifreleme teknikleri

Internet Tarihçe

1961-1972: İlk packet-anahtarlama prensipleri

- 1961: Kleinrock - queueing theori packet-anahtarlamanın etkinliğini gösterdi
- 1964: Baran - packet-anahtarlama (askeri ağlarda)
- 1967: ARPAnet (Advanced Research Projects Agency)
- 1969: ilk ARPAnet düğümü çalışıyor

- 1972:
  - ARPAnet halk demosu
  - NCP (Network Control Protocol) ilk host-host protokolü
  - ilk e-mail programı
  - ARPAnet 15 düğüme sahip



THE ARPA NETWORK

Internet Tarihçe

1972-1980: Ağlar arası bağlantı, yeni ağlar

- 1970: ALOHAnet uydu ağı (Hawaii)
- 1974: Cerf and Kahn – ağları bağlama mimarisi
- 70'lerin sonları: sabit uzunluklu paket anahtarlama (ATM oluşuyor)
- 1979: ARPAnet 200 düğümde

Cerf and Kahn's internetworking principles:

- Ağları bağlamak için ağ içinde bir değişikliğe gerek yok
- Elinden gelenin en iyisini yapan (best effort) servis modeli
- Durum kaydetmeyen yönlendiriciler
- Dağınık kontrol

bugünün internet mimarisini tanımlıyor

Internet Tarihçe

1980-1990: yeni protokoller

- 1983: TCP/IP
- 1982: smtp
- 1983: DNS
- 1985: ftp
- 1988: TCP

- 100,000 host ağlara bağlı

Internet Tarihçe

1990, 2000's: Serbest kullanım, Web, yeni uygulamalar

- 1990'ların başı: ARPAnet artık yok
- Web
  - hypertext [Bush 1945, Nelson 1960's]
  - HTML, HTTP: Berners-Lee
  - 1994: Mosaic, sonra Netscape
  - 1990'ların sonu: e-ticaret

1990'ların sonu – 2000'ler:

- Daha etkili uygulamalar: chat, P2P dosya paylaşımı
- Ağ güvenliği uygulamaları
- tahmini. 50 milyon host, 100 milyon+ kullanıcı
- Ana hatlar Gbps larda çalışıyor

Internet Tarihçe

2007:

- 500 milyon host
- IP üzerinden Ses, Video
- P2P uygulamaları: BitTorrent (dosya paylaşımı) Skype (VoIP)
- Başka uygulamalar: YouTube,
- kablosuz, gezinebilirlik

Giriş: Özet

"bir ton" malzeme işledik!

- Internete bakış
- protokol
- Ağ ucu, merkezi, erişim ağı
  - paket-anahtarlama devre-anahtarlama
  - Internet yapısı
- performans: kayıp, gecikme, throughput
- Katmanlar
- Servis modelleri
- güvenlik
- tarihçe

Şu anda:

- içerik, ve bilgisayar ağlarının ne olduğu hakkında bilgi sahibisiniz
- Detaylar geliyor ☺!