

# DoS attacks

## Een serieuze dreiging?

Marijn Swenne

# Inhoud

- Wat is een Denial of Service (DoS) aanval?
- Typen DoS aanvallen
- Manieren van uitvoeren DoS aanval
- Conclusie

# Wat is een Denial of Service (DoS) aanval?

- Onbereikbaar maken van een service voor legitieme gebruikers
- Geen inbraak

# Een aantal feiten

- Meer dan 4000 DoS aanvallen tegen bedrijven per week
- Zeer moeilijk tegen te beveiligen
- Minder kosten belangrijker dan veilig

# Een paar voorbeelden

- Februari 2000 -> Amazon.com, CNN, Yahoo! en eBay
- Meer dan 1.000.000.000 \$ schade

# Een paar voorbeelden

- Mei 2001 -> GRC.COM
- Dader claimt een 13 jarige te zijn

# Een paar voorbeelden

- Oktober 2002 -> Root DNS servers
- Van de 13 root DNS servers werden er:
  - 7 onbereikbaar, 2 moeilijk bereikbaar, 4 bereikbaar
- Grootste DoS tegen Internet ooit?
- Aanval mislukt...

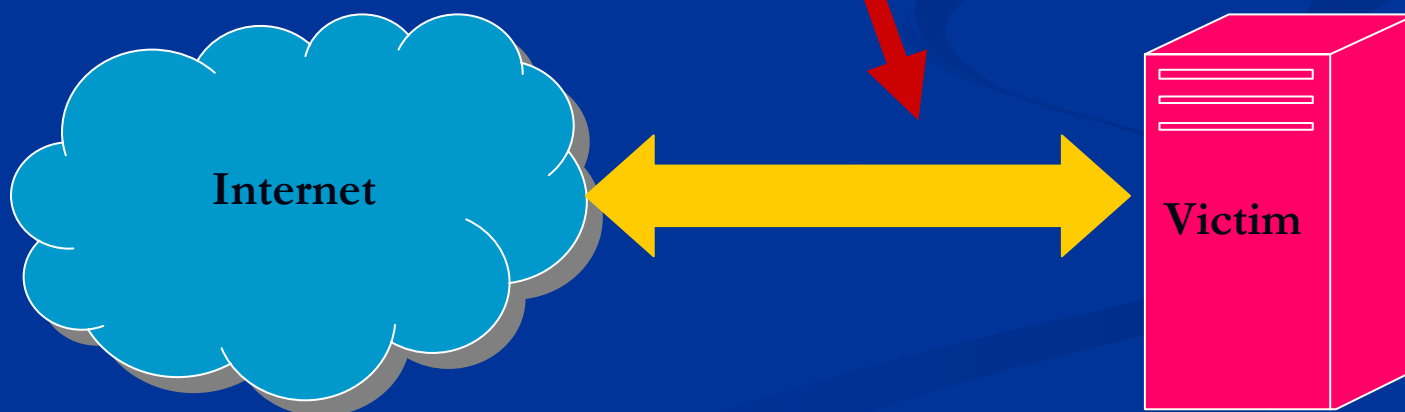
# Een paar voorbeelden

- Oktober 2004 -> Overheid.nl en Kabinet.nl
- Aanslag opgeëist door 0x1fe -> hoofdverdachte voor het gerecht gedaagd (enkele 10Keuro's).

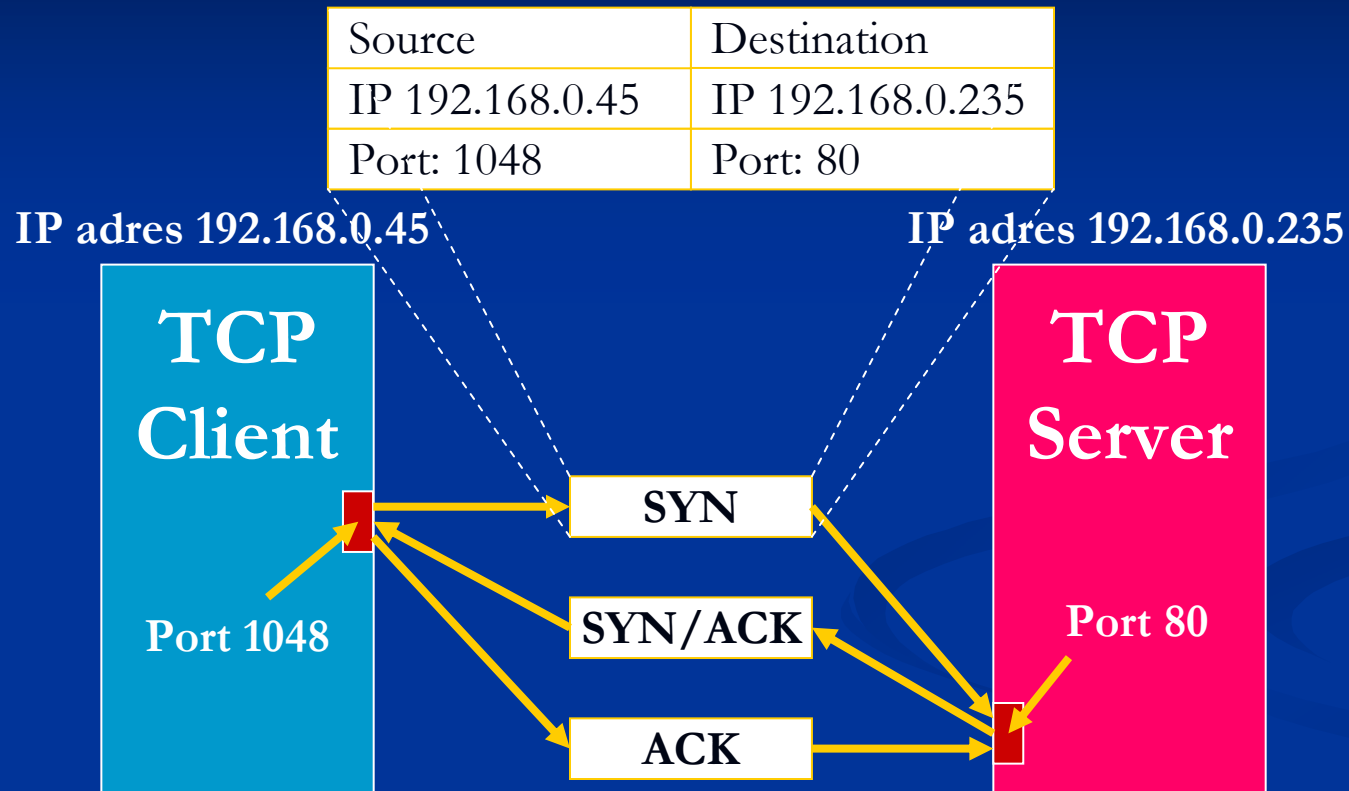


# Type DoS aanvallen

- Overspoelen van computer resources
- Overspoelen van netwerk resources
- Misbruik van zwakte in communicatie protocol
- Fysiek verbinding verbreken

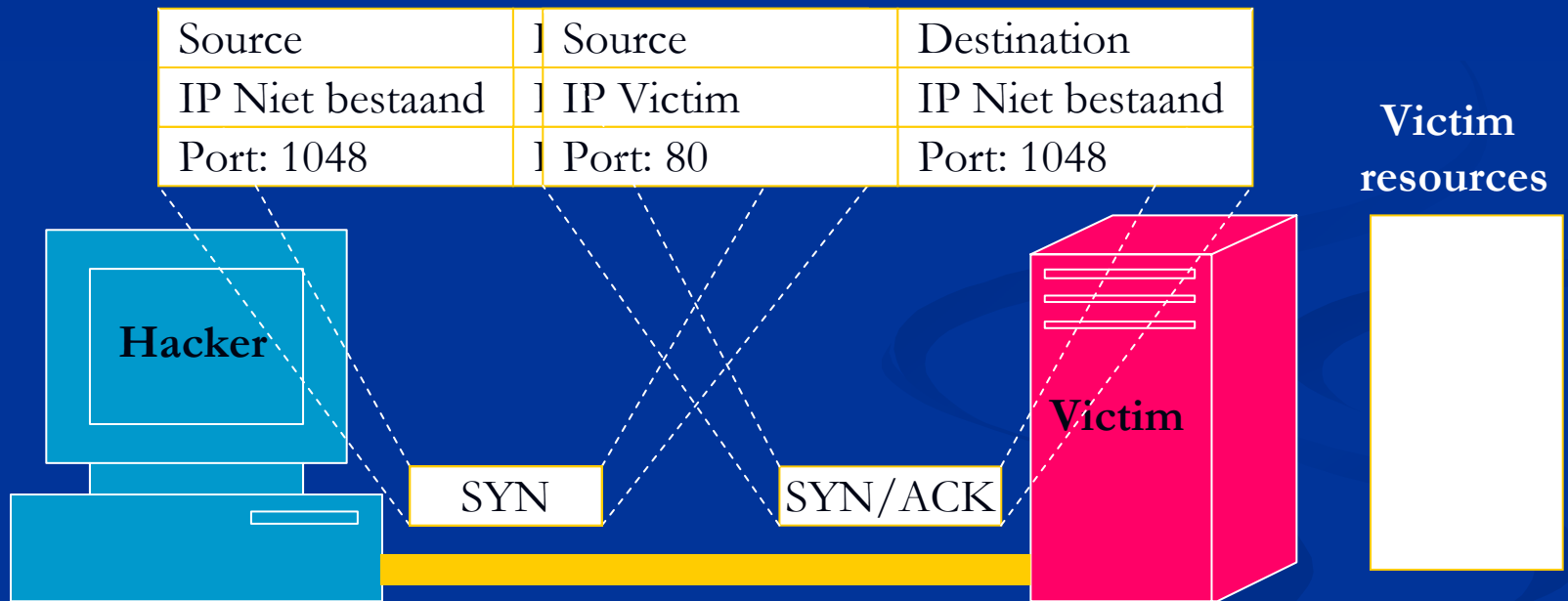


# Het opzetten van TCP connecties



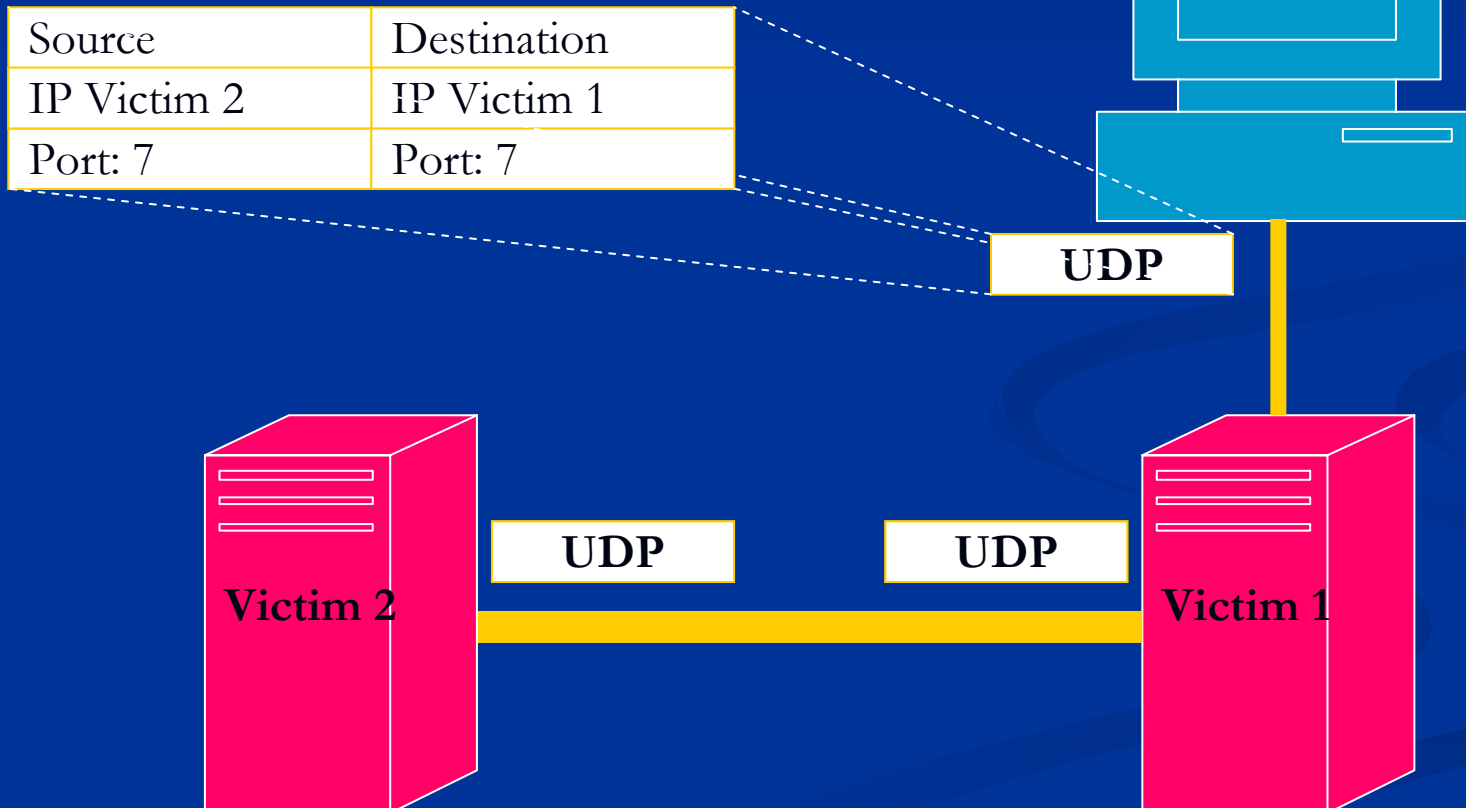
# Overspoelen van computer resources

## ■ SYN flood



# Overspoelen van bandbreedte

## ■ UDP looping



# Misbruik van zwakte in protocol

## ■ Teardrop Attack



# Fysiek verbinding verbreken



# Manieren van uitvoeren DoS aanval

- Denial of Service (DoS)

# Denial of Service (DoS) c. 1990



Hoeveelheid verkeer is afhankelijk van  
de internetverbinding van de Hacker



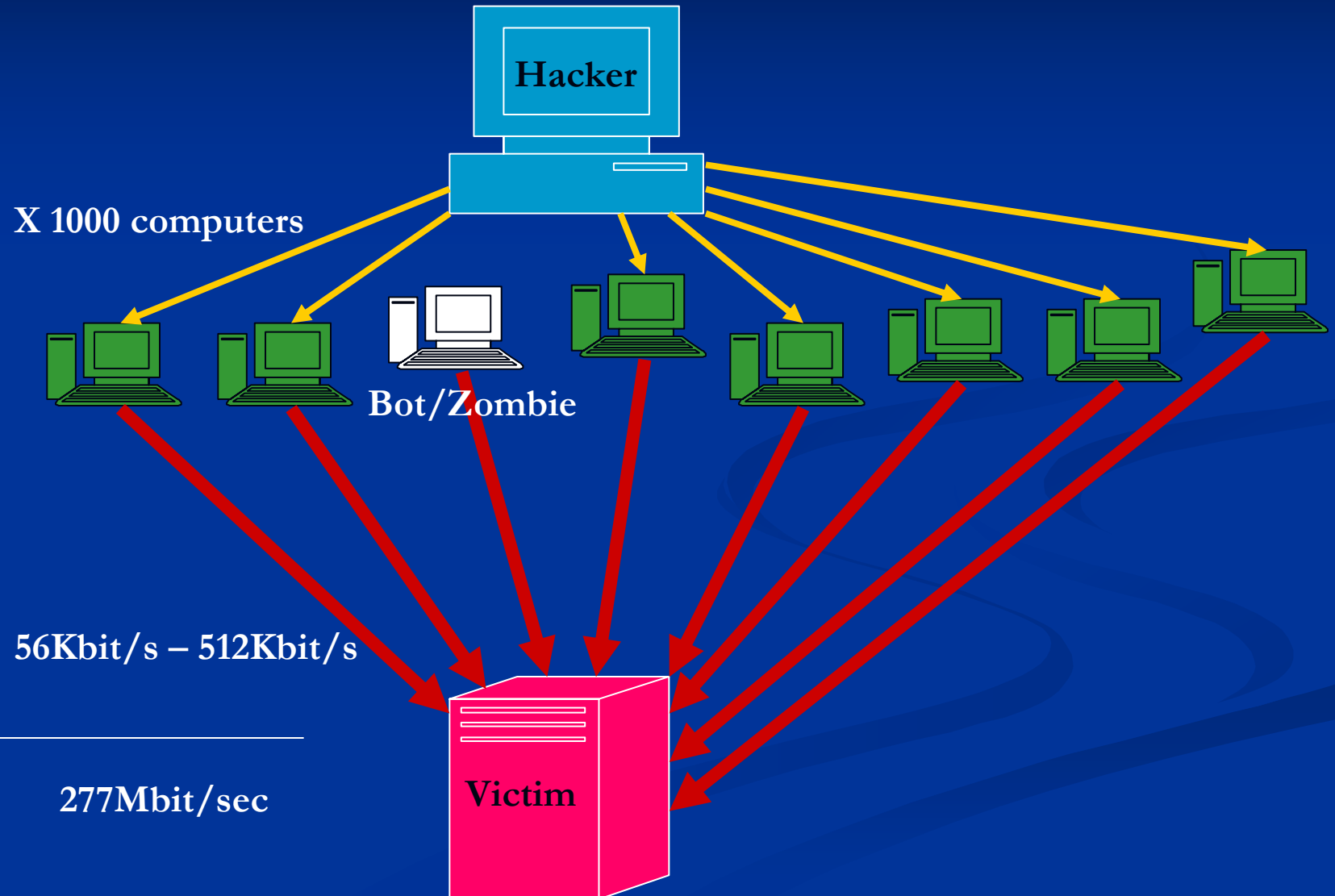


# Manieren van uitvoeren DoS aanval

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)

# Distributed Denial of Service (DDoS)

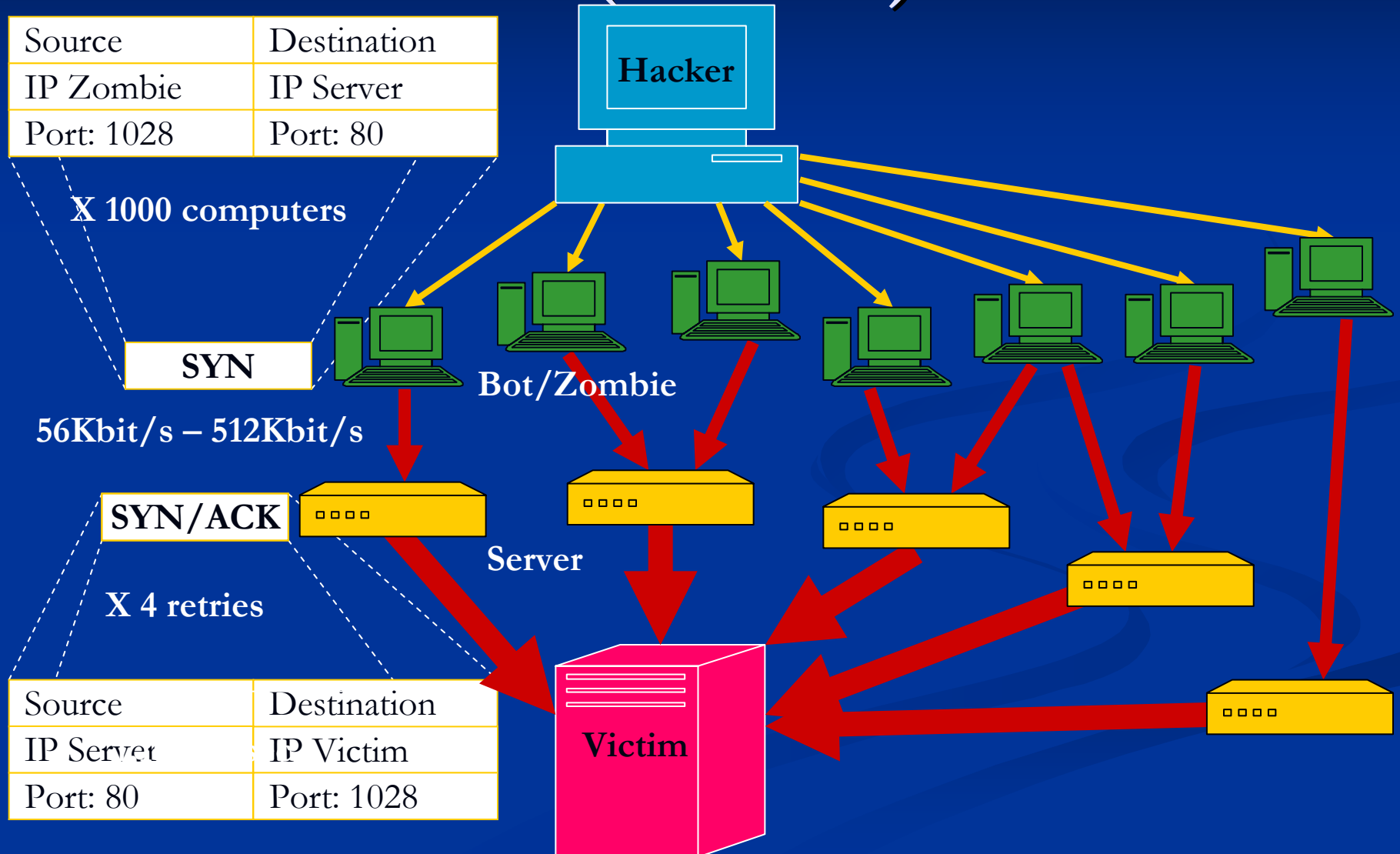
1999



# Manieren van uitvoeren DoS aanval

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Distributed Reflection Denial of Service (DRDoS)

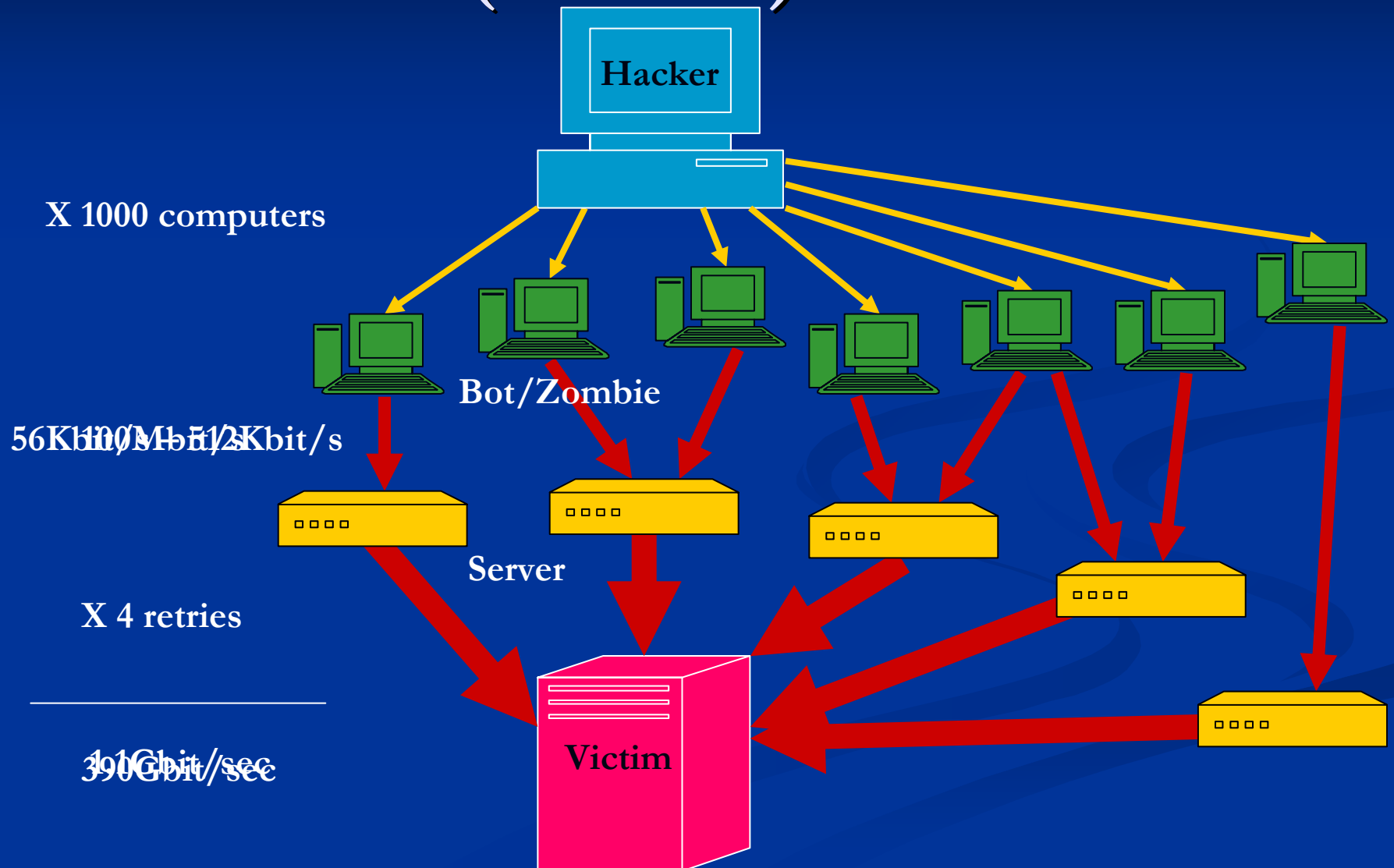
# Distributed Reflection Denial of Service (DRDoS) 2002



# Manieren van uitvoeren DoS aanval

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Distributed Reflection Denial of Service (DRDoS)
- Distributed Reflection Denial of Service (DRDoS) vanaf Grid

# Distributed Reflection Denial of Service (DRDoS) vanaf Grid



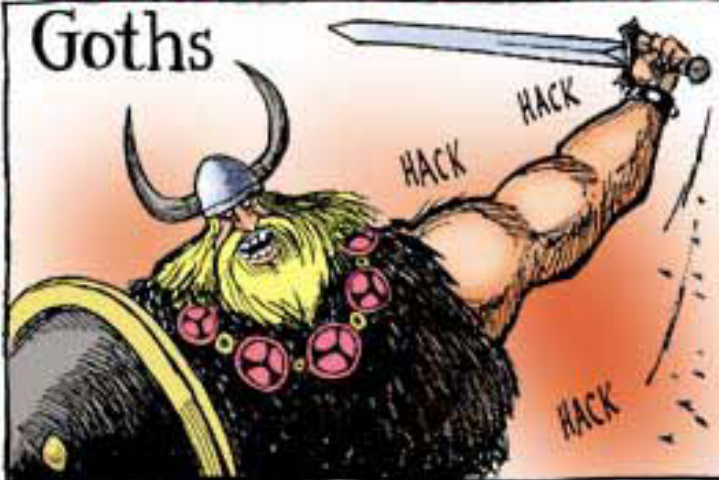
# Conclusie

- Vindt vaak plaats
  - Moeilijk tegen te beschermen
  - Geen hype maar trend
  - In ontwikkeling
- 
- Is een serieuze bedreiging voor bedrijven die internetdiensten aanbieden

# Einde

## BRINGING CIVILIZATION TO ITS KNEES...

Goths



Vandals



Huns



Geeks

