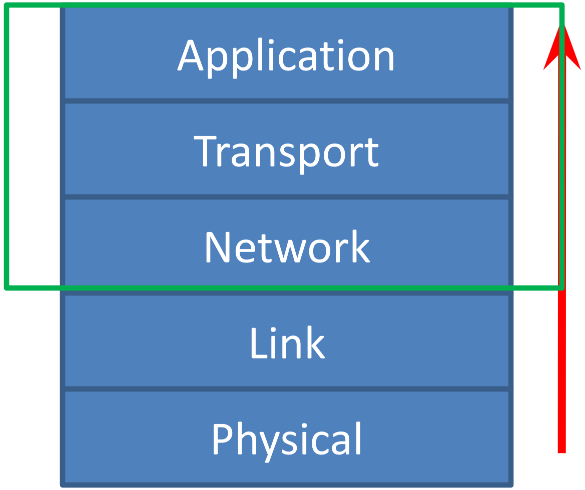
Computer and Network Security: Denial of Service Attacks

Kameswari Chebrolu

Outline

- DOS Basics
- DOS attacks at different layers of the protocol stack
- Solutions to the same



Application

Transport

Network

Link

Physical

Denial of Service (DOS)

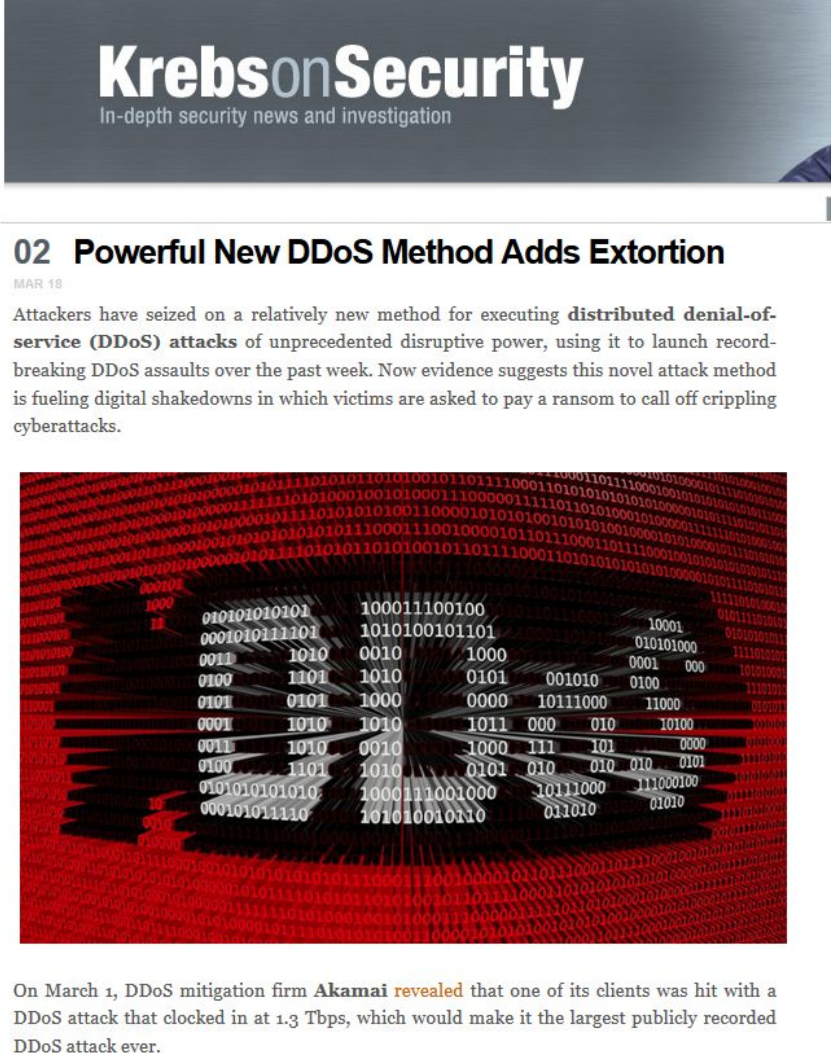
- Prevent users from accessing machines or network resources
  - Do it with little computing work
- Why do it?
  - Extortion (pay ransom else we will bring your service down)
  - Competition
  - Political
  - Warfare

Extent of Use

Black Market

Service	Price
50,000 botnets for rent for two weeks	$4000
DDOS for one week/hour	$150/$10

As Extortion



KrebsonSecurity

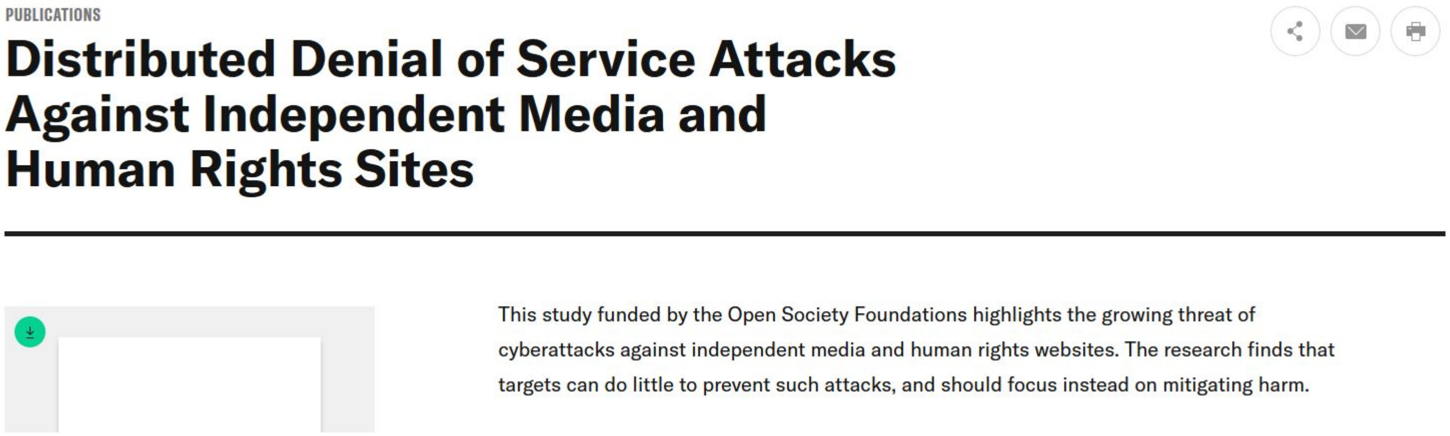
In-depth security news and investigation

02 Powerful New DDoS Method Adds Extortion

MAR 18

Attackers have seized on a relatively new method for executing **distributed denial-of-service (DDoS) attacks** of unprecedented disruptive power, using it to launch record-breaking DDoS assaults over the past week. Now evidence suggests this novel attack method is fueling digital shakedowns in which victims are asked to pay a ransom to call off crippling cyberattacks.

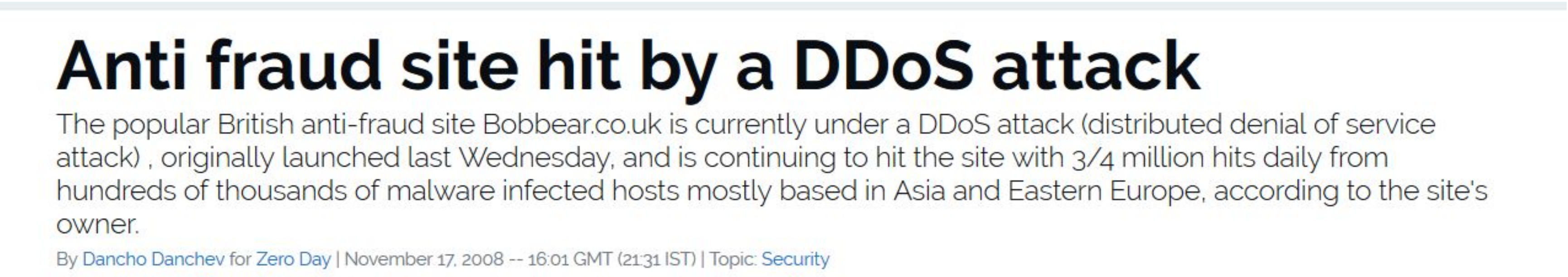
On March 1, DDoS mitigation firm **Akamai** revealed that one of its clients was hit with a DDoS attack that clocked in at 1.3 Tbps, which would make it the largest publicly recorded DDoS attack ever.



PUBLICATIONS

Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

This study funded by the Open Society Foundations highlights the growing threat of cyberattacks against independent media and human rights websites. The research finds that targets can do little to prevent such attacks, and should focus instead on mitigating harm.



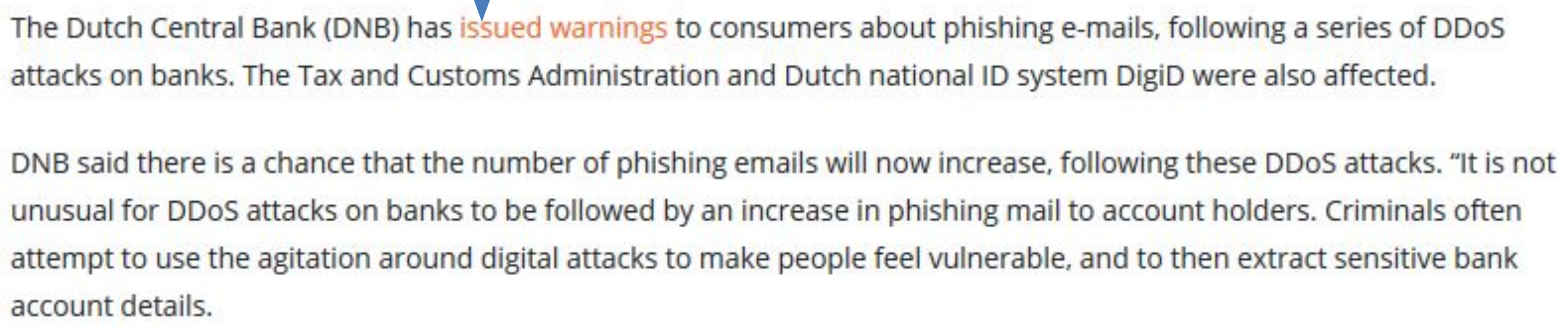
Anti fraud site hit by a DDoS attack

The popular British anti-fraud site Bobbear.co.uk is currently under a DDoS attack (distributed denial of service attack) , originally launched last Wednesday, and is continuing to hit the site with 3/4 million hits daily from hundreds of thousands of malware infected hosts mostly based in Asia and Eastern Europe, according to the site's owner.

By Dancho Danchev for Zero Day | November 17, 2008 -- 16:01 GMT (21:31 IST) | Topic: Security

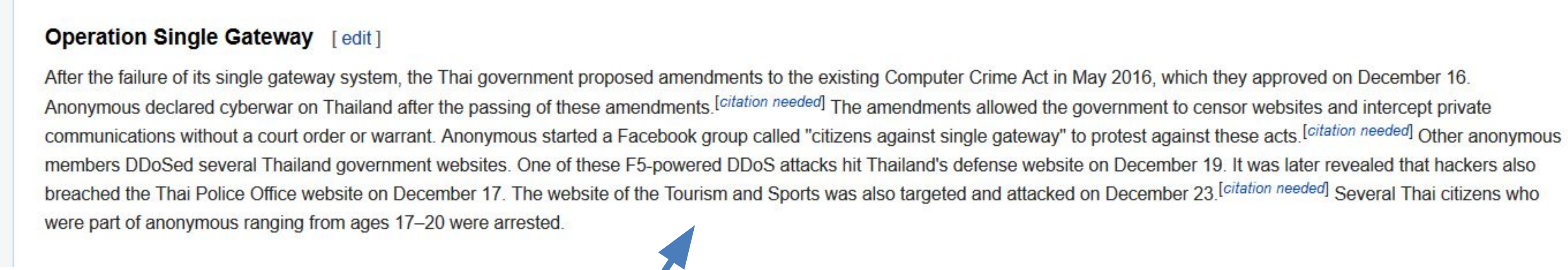
Bring down enemies

DDOS make phishing email look real: Email explains outage and offers alternate URL



The Dutch Central Bank (DNB) has issued warnings to consumers about phishing e-mails, following a series of DDoS attacks on banks. The Tax and Customs Administration and Dutch national ID system DigiD were also affected.

DNB said there is a chance that the number of phishing emails will now increase, following these DDoS attacks. “It is not unusual for DDoS attacks on banks to be followed by an increase in phishing mail to account holders. Criminals often attempt to use the agitation around digital attacks to make people feel vulnerable, and to then extract sensitive bank account details.

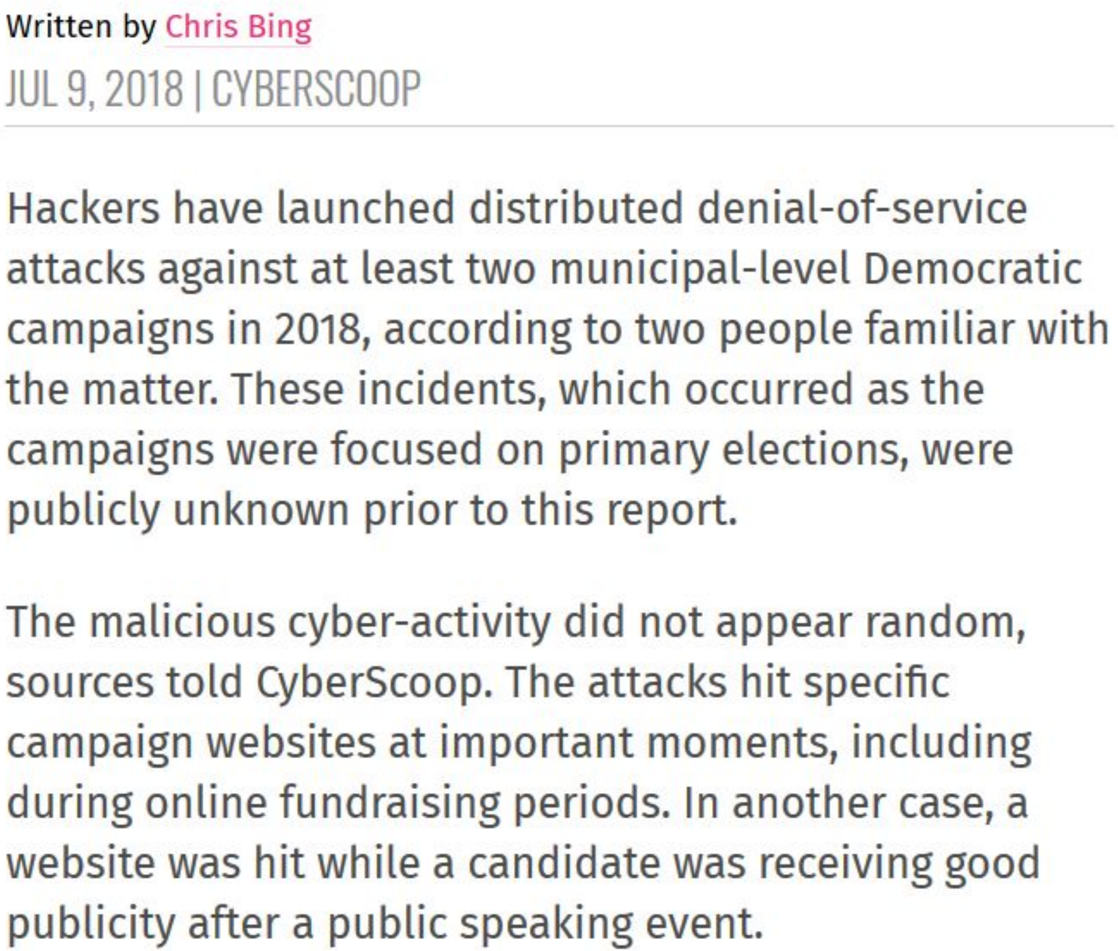


Operation Single Gateway [edit]

After the failure of its single gateway system, the Thai government proposed amendments to the existing Computer Crime Act in May 2016, which they approved on December 16. Anonymous declared cyberwar on Thailand after the passing of these amendments.[citation needed] The amendments allowed the government to censor websites and intercept private communications without a court order or warrant. Anonymous started a Facebook group called "citizens against single gateway" to protest against these acts.[citation needed] Other anonymous members DDoSed several Thailand government websites. One of these F5-powered DDoS attacks hit Thailand's defense website on December 19. It was later revealed that hackers also breached the Thai Police Office website on December 17. The website of the Tourism and Sports was also targeted and attacked on December 23.[citation needed] Several Thai citizens who were part of anonymous ranging from ages 17–20 were arrested.

Activism

Elections



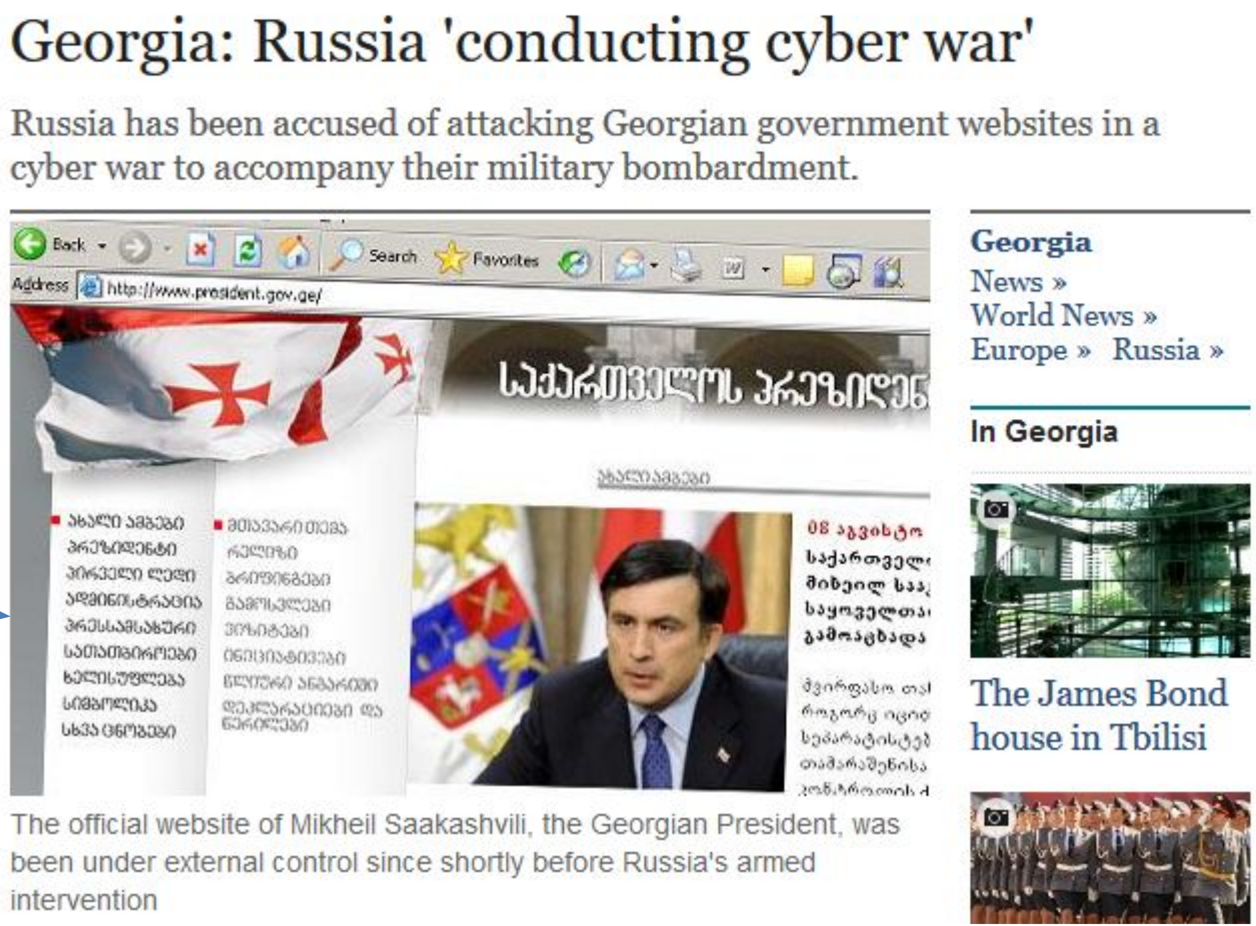
Written by Chris Bing

JUL 9, 2018 | CYBERSCOOP

Hackers have launched distributed denial-of-service attacks against at least two municipal-level Democratic campaigns in 2018, according to two people familiar with the matter. These incidents, which occurred as the campaigns were focused on primary elections, were publicly unknown prior to this report.

The malicious cyber-activity did not appear random, sources told CyberScoop. The attacks hit specific campaign websites at important moments, including during online fundraising periods. In another case, a website was hit while a candidate was receiving good publicity after a public speaking event.

CyberWar



Georgia: Russia 'conducting cyber war'

Russia has been accused of attacking Georgian government websites in a cyber war to accompany their military bombardment.

The official website of Mikheil Saakashvili, the Georgian President, was been under external control since shortly before Russia's armed intervention

Georgia
News »
World News »
Europe » Russia »

In Georgia

The James Bond house in Tbilisi

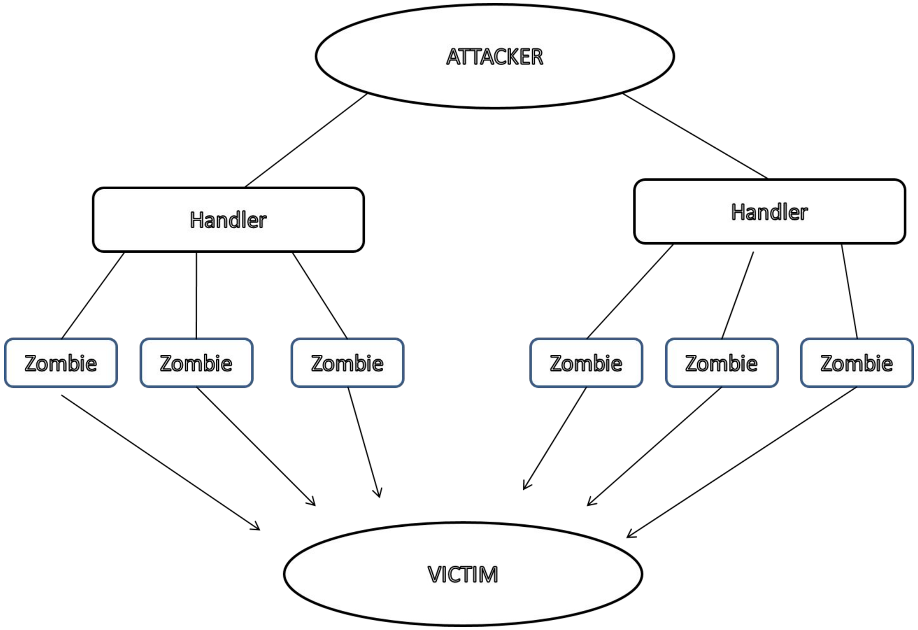
Types of DOS

- **Network** (our focus): Target bandwidth or processing capacity
  - Typically involves some form of flooding

  (Crashing system due to protocol implementation bug also possible)
- OS: Exhaust resources
  - Use up all disk space, open zillions of files, spawn zillions of processes
  - Defense: Isolation
- Software: Crash program/system
  - Supply input that crashes the program
  - Defense: Careful testing

Other Aspects

- Source IP address often spoofed
- Distributed DOS:
  - Leverages resources of multiple machines to overwhelm a powerful server
  - Botnets available for rent cheaply
  - Very difficult to stop (filtering difficult)
  - Yahoo, Amazon, Google all have been subject to it
- Current Internet not designed to handle DDOS



Botnet

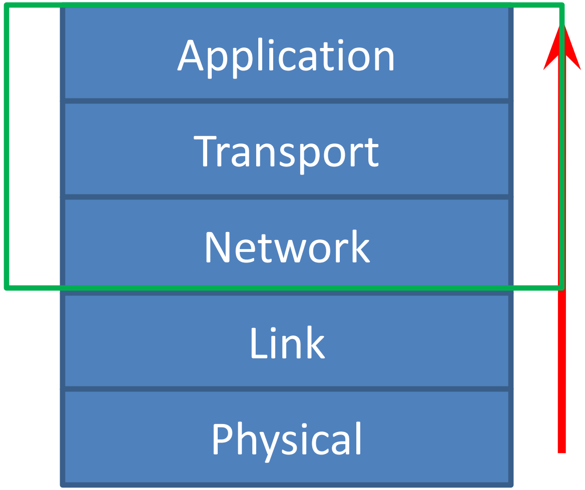
Details

- Goal: Bring down a popular website
- What to attack? Bottleneck link or bottleneck process
- 1kbps = 1pkt /sec * 1000 bits = 100pkt/sec * 10 bits
- Bottleneck link: saturate link with least effort
  - Go for large packet size (and less per packet rate)
- Bottleneck process: Overwhelm the process with work
  - Go for high per packet rate (and min sized packet to maximize rate)

- How to defend?
  - Discard packets from the attacker’s IP (filter in the firewall)
  - Attacker will spoof different source IPs. Then?
    - Not much can be done by the target
    - ISP may filter out those packets though (Ingress filtering)
  - Attacker will launch DDOS attack from compromised machines. Then?
    - How many compromised machines are required? Try to make it large but not always possible
    - Not a level playing field (attacking often takes less effort than defense)

Outline

- DOS Basics
- DOS attacks at different layers of the protocol stack
- Solutions to the same



Application

Transport

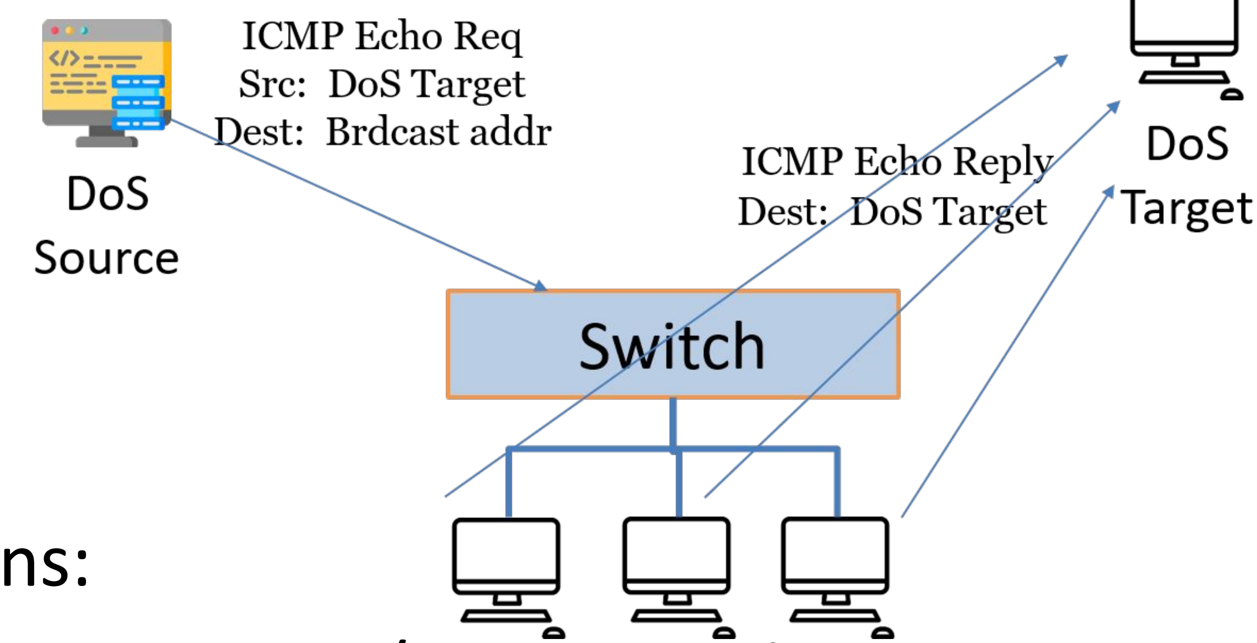
Network

Link

Physical

Network Layer Attacks

- ICMP Ping Flood:
  - A powerful machine overwhelms a weaker machine with ICMP echo requests (Ping requests)
  - Weak machine drops other valid connections
- Smurf Attack:
  - A clever variation that amplifies the attack (DDOS)
  - ICMP request
    - packet source: victim/target; destination: broadcast
  - All hosts in the subnet will reply to the victim and overwhelm it

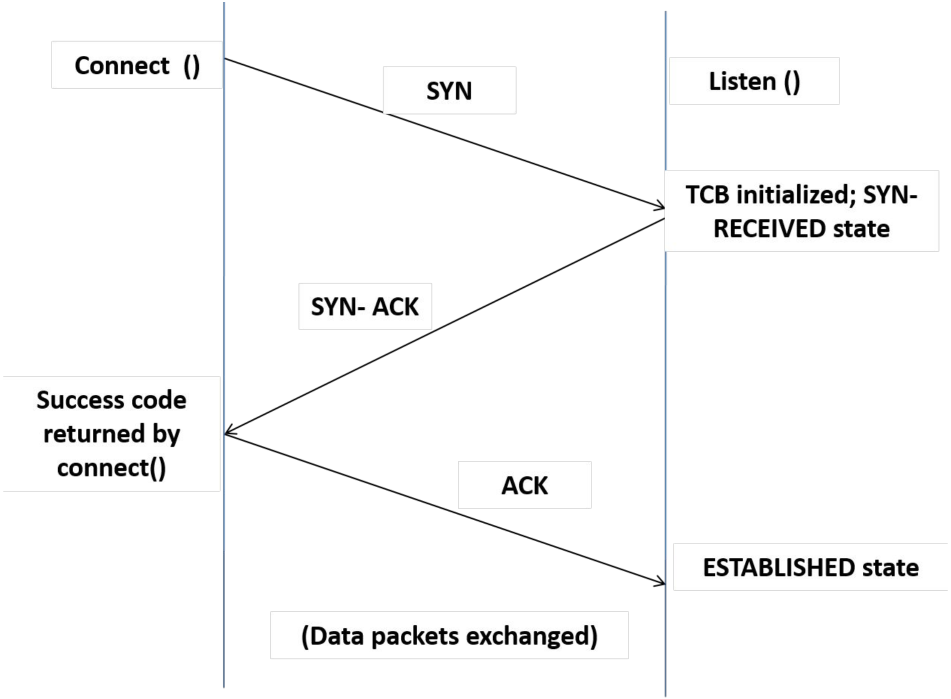


Solutions:

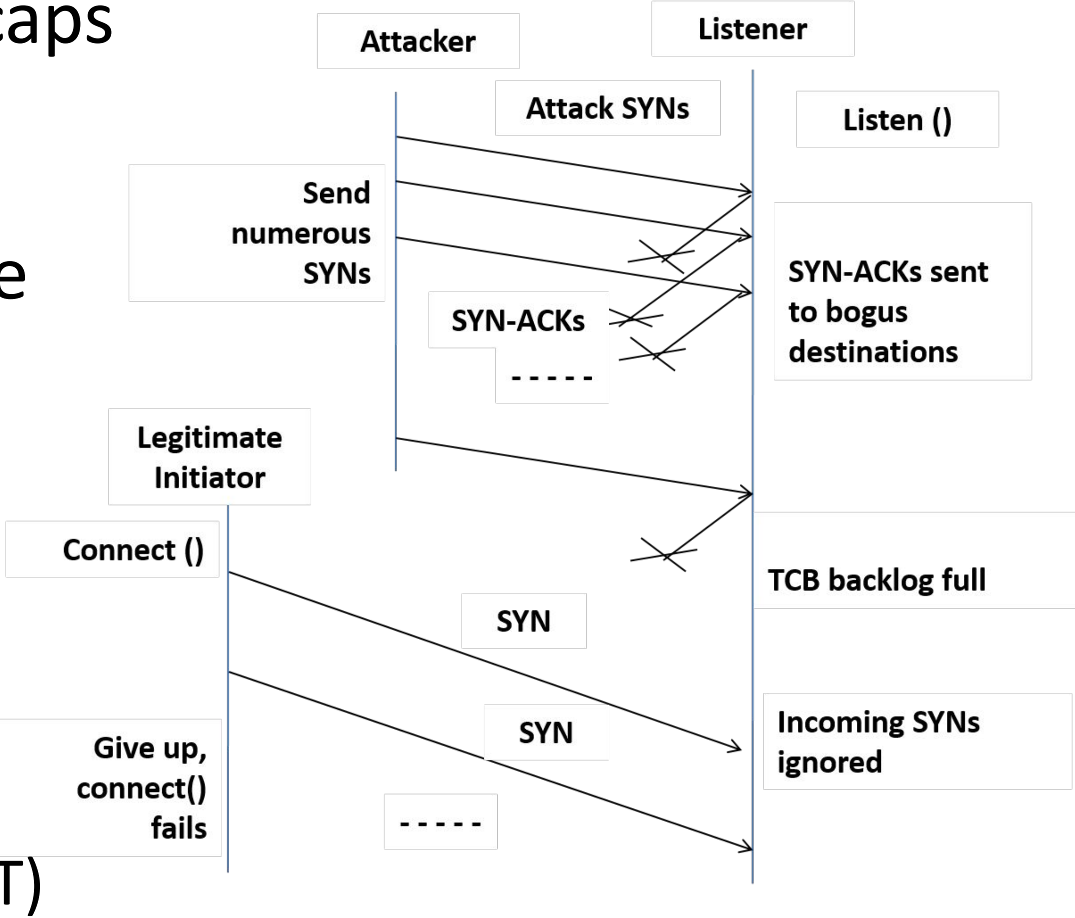
- Configure server/routers to drop ping requests
- Host/Routers should ignore broadcast requests
- Routers should also not forward such requests

Transport Layer Attacks

- TCP SYN Flood Attack
  - Receipt of SYN creates Transmission Control Block (TCB) data structure
  - TCB's range from 300-1400 bytes depending on OS, options etc
  - Potential for memory exhaustion DOS



- “Backlog" parameter: caps number of TCBs simultaneously in the SYN-RECEIVED state
  - Timer to reap memory
- Source IP Properties:
  - Spoofed
  - Different addresses (to avoid filtering)
  - Non-existent machine (don’t respond with RST)



MS Blaster

- Launched in August 2003
- A worm that spread exploiting buffer overflow on windows system (to be covered later)
- Payload: launch a TCP SYN flood attack against port 80 of windows-update server
- MS solution: Change server name and used Akamai to deliver updates

Detecting SYN flood attacks

- SYN from random spoofed address □ SYN/ACKs to non-existing IPs
- Backscatter measurements: listen to unused IP address space (via a network telescope)
  - Extrapolate extent of attacks based on observation
  - Example: 2001: ~400 attacks/week ; 2008: ~4000 syn attacks/day
- https://www.caida.org/projects/network_telescope

Defense

Host based

- Increase backlog: does not help, attacker will scale SYNs
- Reduce Timer: Reaps TCB after this time
  - Can reap legitimate connections also
  - Attacker can time SYNs accordingly
- Identify the attacker and drop connections
  - Hard since attacker can spoof source addresses
  - Also easy to launch since handshake needs no completion

Defense

Host based

- Avoid state. Buy how?
  - Modify TCP protocol □ client changes are not easy
- SYN Cookies: Maintain zero state
  - Connection state encoded into Seqno of SYN-ACK. How?
    - 5 bits: timestamp (counter incremented every minute modulo 32)
    - 3 bits: maximum segment size
    - 24 bits: keyed hash of server/client IP addresses/port and timestamp
  - On receipt of seqno in ACK, TCB state can be regenerated

- SYN Cookies:
  - Implemented in many linux distributions
  - Attacker now needs to complete handshake □ more resources
    - For example, can’t use random spoofed IP addresses
  - Drawbacks:
    - Not all TCB data can be compressed into 32-bit seqno; especially options
    - Handshake ACK lost ? SYN-ACKs cannot be retransmitted (requires state)

Network based

- Ingress filtering: ISPs drop spoofed packets
  - Src IP address does not belong to the domain
  - May not be ubiquitous
- Buy a reverse-proxy service from a cloud provider (e.g. Prolexic proxy from Akamai)
  - Replies to SYNs and forwards only established connections to website
  - 20k bot-army can generate 2Gbps; Proxy can handle 20Gbps

TCP connection Flood

- A powerful botnet can complete TCP handshake and send small GET request (and repeat)
  - Syn cookies and proxy help? No
  - If a signature (pattern) can be found, proxy can rate limit/block
- Can attacker use random source IP?
  - No □ bots location revealed

Optimistic TCP ACK Attack

- Congestion Control: Sending rate dictated by ACKs
- Attacker sends ACKs of packets before they are received □ increases sending rate of this connection □ no bandwidth left to serve others

Optimistic TCP ACK Attack

- Launched against many servers, can overwhelm a common router serving them
- Defense: Limit maximum rate of a connection; block connections that appear to launch DOS

Application Layer Attacks

- Leverage hundred/thousands of servers spread across the world providing a service
- Rely on some form of amplification
  - Reply from server is generally much bigger than request to server
- Spoof source □ set source of request to victim (much like in smurf attack)

Application Layer Attacks

- DNS Amplification Attack
  - Reply is generally much bigger than request (e.g. 60 bytes vs 4096 bytes); more so with DNSSEC
  - Attacker spoofs DNS request to open DNS resolvers (thousands of such resolvers)
    - Request source is the target IP
    - Small attacker packets yields large flood
  - Some attacks known to cause as much as 300Gbps DDOS
- Difficult to block at target since sources are legitimate DNS servers
- Ingress filtering can help but not universal

- NTP (Network Time Protocol) amplification
  - Server used by machines to set clocks; lakhs of such servers
  - Similar to DNS amplification, but much worse
  - Request: return the addresses of up to the last 600 machines that the NTP server has interacted with
  - Request of 234 bytes can generate a response of 48k bytes
  - Just contacting 4000 servers can yield a 400Gbps DDOS
- Ingress filtering can help but not universal

- Memcached amplification (2018)
  - Memcached: popular, open-source, distributed caching system; runs on UDP and TCP
    - Used to scale web applications; facebook, twitter, youtube, github all use it
  - Attack: Target unprotected Memcached servers operating on UDP; use spoofed IP address that matches the victim's IP
  - 1.3/1.7 Tbps attack against GitHub and other unidentified site
    - 51,000+ amplification; 15-byte request result in a 750kB response
    - 88,000 open Memcached servers; about 5700 were exploited
- Disable UDP; rate limiting of UDP traffic
- Ingress filtering can help but not universal

Other Aspects

- Overwhelm application’s processing capacity
- Issue requests that require heavy processing (trigger worst case complexity)
  - Server process is the bottleneck
- Defense:
  - Only authorized users can perform expensive operations or charge for the same
    - Authorization itself can count as an expensive operation ☹
  - Over provision resources (e.g. more CPU cores)
    - Very expensive proposition; attacker will scale up the attack

Defense: IP Traceback

- In DOS attack useful to determine the ‘actual’ origin of spoofed packet to take action
  - Attempt at source authentication
- Solution: Routers log details of all packets forwarded
  - Lot of space, global coordination
- Another Solution: Packet Marking
  - Embed info in packet to deconstruct the path

Packet Marking

- Naïve approach: Each router that forwards the packet appends its address to it
  - Packet can get fragmented
  - Slows down the routers
- Node sampling:
  - Designate one field in the packet for marking
  - Each router probabilistically overwrites field with probability p
  - How is the path to source constructed then?

- Routers closer to victim have higher probability of marking
  - Nearest router p; second-nearest router (1-p)p
  - Compute expected number and correlate with received marked packets
- Not seen widespread use
  - Requires support from routers
- IPSec better solution
  - Provides authentication, confidentiality, integrity and much more

Statistics

- https://blogs.akamai.com/2019/01/a-look-back-at-the-ddos-trends-of-2018.html (and)
- https://securelist.com/ddos-report-q2-2019/91934/

Summary

- DOS: Prevent users from accessing machines or network resources
  - DDOS: distributed to pool in more resources; circumvent security mechanisms like filtering
- Variety of DOS attacks possible at various layers of the stack
  - Solutions don’t always solve it effectively
- Current Internet not designed to handle DDOS
  - Various attacks keep happening