Carnegie Mellon CyLab
4616 HENRY STREET
PITTSBURGH, PA 15213
PH: (412) 268-7195
FX: (412) 268-7196
www.cylab.cmu.edu

The Coremelt Attack

Ahren Studer and Adrian Perrig

We've Come to Rely on the Internet

- Critical for businesses
  - Up to date market information for trading
  - Access to online stores
    - One minute down time = loss of €13,000
- Critical for utilities
  - Networks relay usage information to producers
    - Absence of communication may lead to permanent damage and potentially cascading faults

Crippling Internet Services: Denial of Service Attacks

- Application Level Attacks
  - Packets prevent legitimate access at the server
- Network Level Flooding Attacks
  - Network-level congestion prevents legitimate access at the network link

Preventing Denial of Service Attacks

Initial defense attempt:

Stop unwanted traffic

- Approaches
  - Filter malicious packets, patch software
  - Identify the source of unwanted traffic
  - Provide desired traffic with network capabilities, routers will prioritize packets with capabilities

CyLab www.cylab.cmu.edu Carnegie Mellon

If Defenses are Deployed, Then:

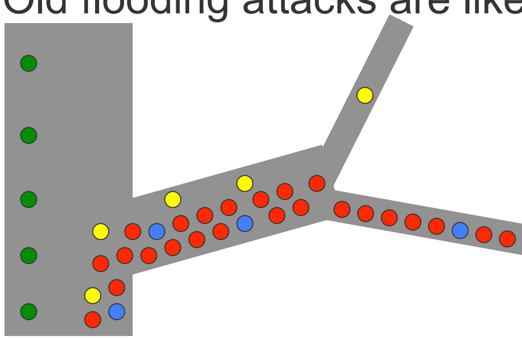
- Independent of malicious parties' resources
  - Malicious packets stopped
  - Server resources are available to legitimate traffic
  - Legitimate traffic can reach the server

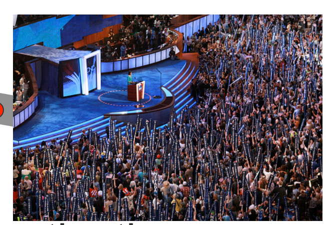
- What could malicious parties do once they are unable to attack the server or its link?

CyLab www.cylab.cmu.edu Carnegie Mellon

Road Networks

- Old flooding attacks are like protestors

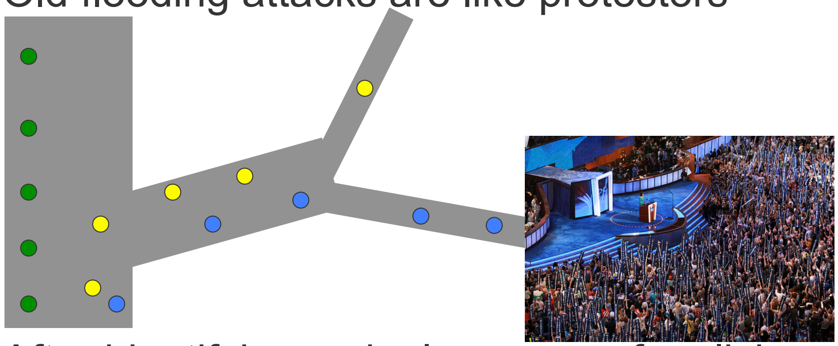




- Limited capacity near the destination causes congestion

Road Networks

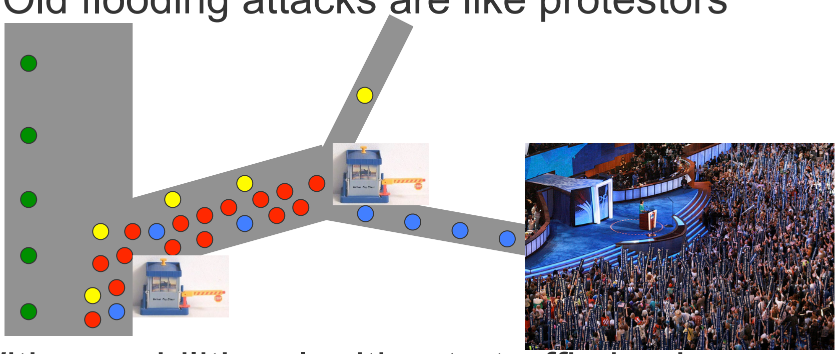
- Old flooding attacks are like protestors



- After identifying a single source of malicious traffic, an ISP can “pull the plug”

Road Networks

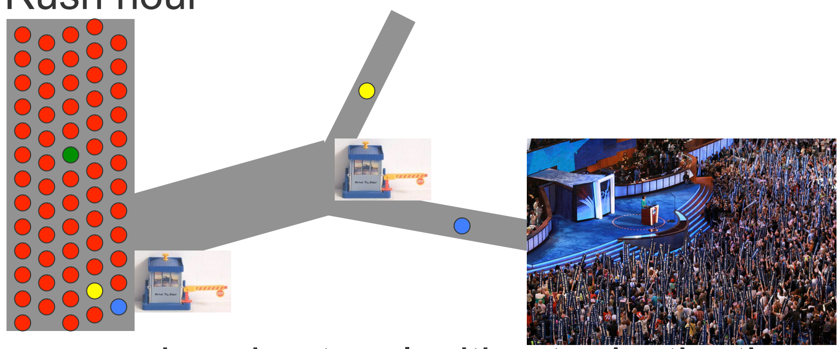
- Old flooding attacks are like protestors



With capabilities, legitimate traffic is given preference

Road Networks

- Rush hour



Everyone is going to a legitimate destination and the major roads just aren't big enough

Back to Networks

- How to cause rush hour on the Internet?
  - Overwhelm backbone link

1. Collect a large number of machines
   - Rent a botnet or two
2. Send enough traffic to a router to cause congestion
   - Not so simple

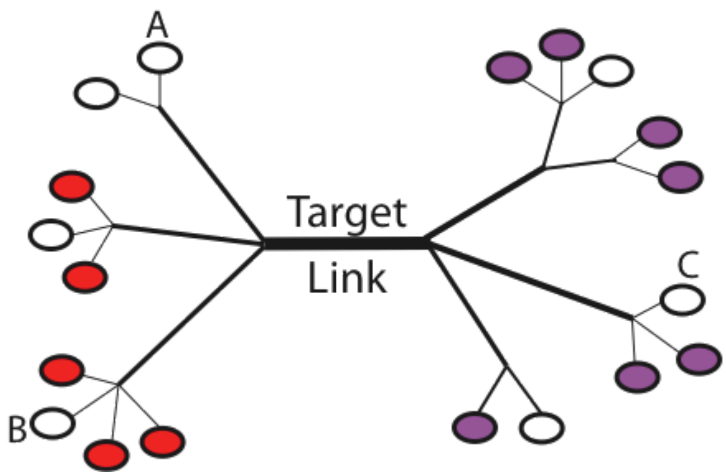
How to Flood a Core Router

- Send traffic to the next router after the target
  - Problem: Filters can drop traffic destined for a router
- Send traffic to a server past the target
  - Problem:, attack traffic will lack capabilities while legitimate traffic will proceed unimpeded

The Coremelt Attack

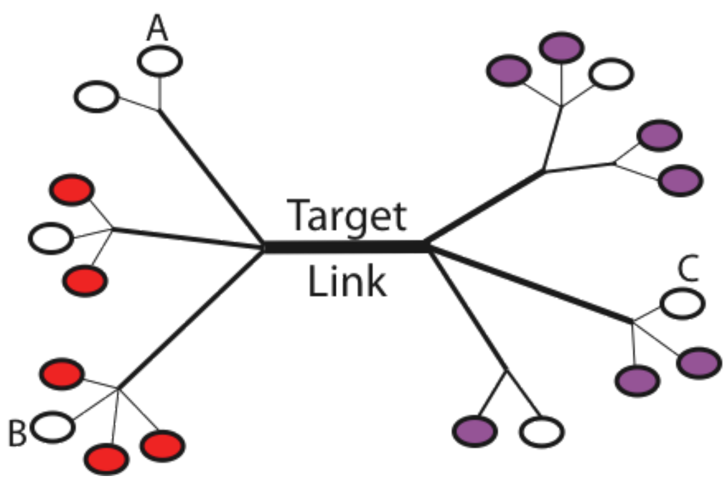
- Bots sending traffic to each other
  - Such that traffic traverses the target link
- Bypasses existing DoS defenses
  - Traffic is “wanted” so capabilities are acquired
  - No obvious reason to filter, looks legitimate
    - Each bot contributes a small amount of traffic

The Coremelt Attack



CyLab
www.cylab.cmu.edu
Carnegie Mellon

The Coremelt Attack



Launching a Coremelt Attack

1. Rent a well distributed botnet
   – With a dense botnet, smaller tributary links will congest first
2. Discover routes that traverse the target
   – Discreet use of traceroute
3. Send "unfriendly" traffic
   – TCP will back off
   – ISPs throttle UDP
   – Send traffic labeled as TCP

Is Coremelt a Threat?

- Can the attack overload core links?
- Can the attack work without clogging other links?
  – Clogging the whole path is unrealistic
  – Collateral damage makes the attack less stealthy
  – Easier to find source of the attack

Simulating Coremelt

- Implementation is expensive & illegal
- Simulation
  - AS level network topology
  - Realistic distributions of subverted machines
  - Varying number of machines
  - Conservative traffic generation capabilities

Network Model

- Graph based on the CAIDA AS dataset
- Treat each AS as a router
- Packets use the shortest route that follows AS routing policies
- AS has limited traffic capacity (internal link)
  - When AS reaches capacity, packets are dropped
  - Target AS dropping packets = Successful attack
  - Other AS dropping packets = Collateral damage

AS Capacity

- Model capacity as a function of AS degree
  - If AS X connects to more networks than AS Y, X should support more traffic than Y
  - Often over provision a link since 100% is rare
  - “Step” model assumes ASes fall into categories

Degree	1	OC-12	601 Mb/s
Degree	2-9	OC-48	2,405 Mb/s
Degree	10-999	OC-192	9,621 Mb/s
Degree	≥ 1000	OC-768	39,813 Mb/s

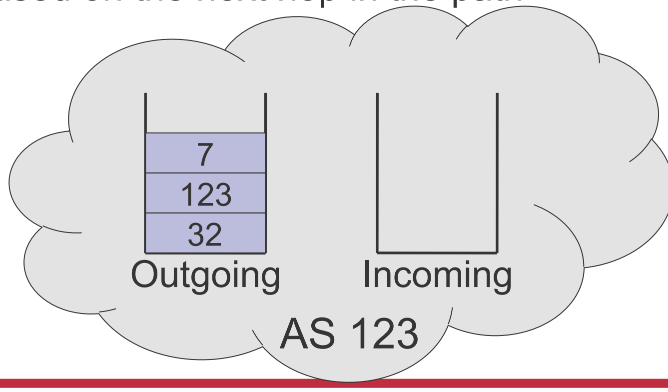
See paper for other models

Attacker Model

- Fixed botnet distributions based on
  - GT-DDoS: flooding attack witnessed at GT
    - Thanks to Chris Lee and Wenke Lee
  - CodeRed: machines seen scanning
- Vary botnet size while maintaining the original botnet distribution
  - # bots in AS = $\lfloor$% of botnet in AS × botnet size$\rfloor$
- Each bot sends packets at 14 or 128 Kb/s

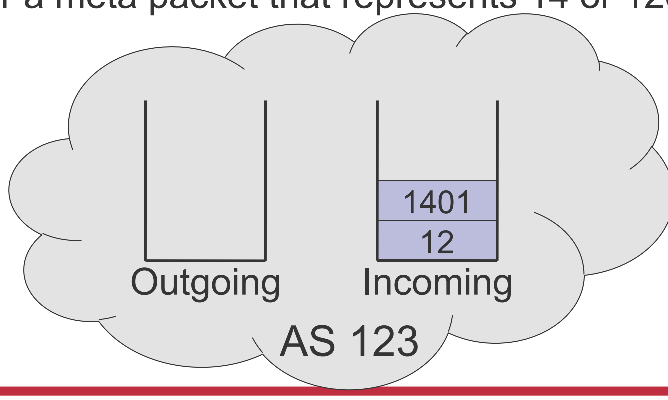
Discrete Simulation of Network

- During Interval i:
  - AS sends packets received during interval i-1 based on the next hop in the path



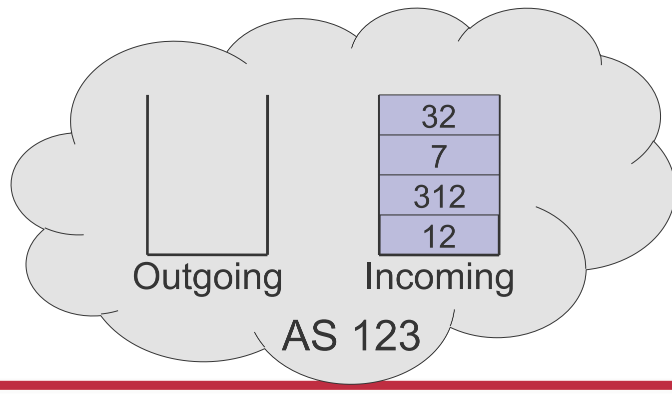
Discrete Simulation of Network

- During Interval i:
  - Each bot in the AS picks a random destination for a meta packet that represents 14 or 128 Kb



Discrete Simulation of Network

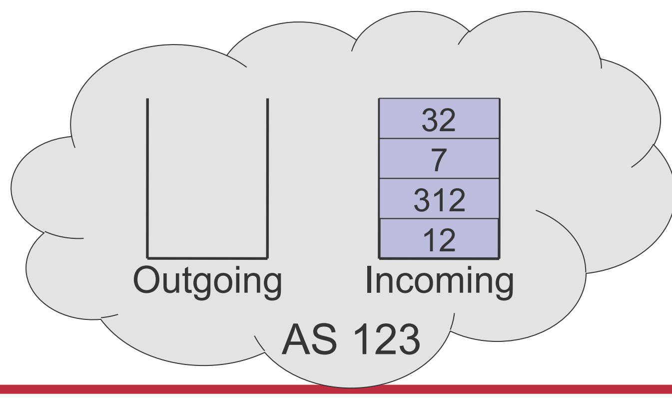
- During Interval i:
  - Other ASes forward traffic to this AS



CyLab
www.cylab.cmu.edu
Carnegie Mellon

Discrete Simulation of Network

- At the end of Interval i:
  - Buffers switch roles for the next interval



Our Metrics

- Destructiveness
  - Fraction of 10 largest ASes that a given attacker can congest

$$\sum_{i=1}^{10} 0.1 \cdot congestAS(i)$$

- Stealthiness
  - Number of collateral ASes congested while attacking the 10 largest ASes

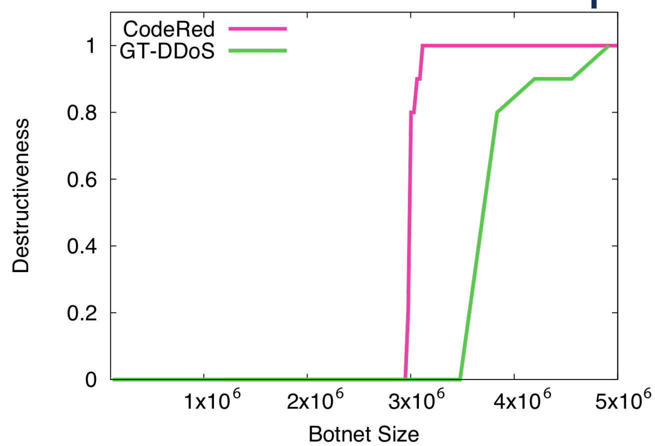
$$\sum_{i=1}^{10} \sum_{j \neq i} congestAS(j)$$

Network and Attacker Numbers

- 30,610 total ASes
  - 11,042 of degree 1: OC-12 (601 Mb/s)
  - 18,083 of degree 2-9: OC-48 (2,405 Mb/s)
  - 1475 of degree 10-999: OC-192 (9,621Mb/s)
  - 10 of degree ≥1000: OC-768 (39,813 Mb/s)
- GT-DDoS: bots in 720 ASes
- CodeRed: bots in 4746 ASes

CyLab
www.cylab.cmu.edu
Carnegie Mellon

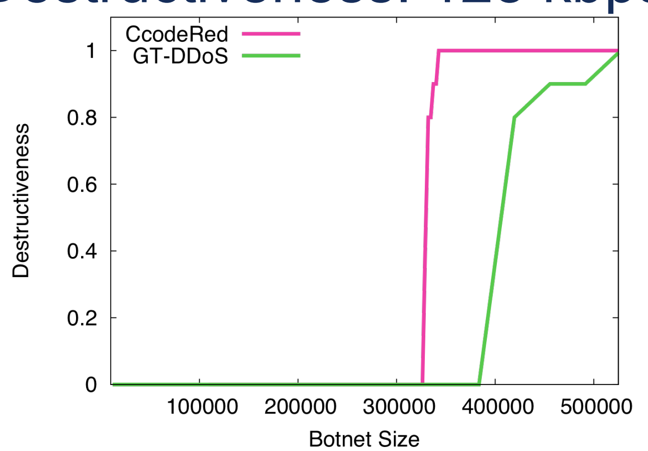
Destructiveness: 14 kbps



- Greater dispersion of bots in CodeRed improves success of Coremelt

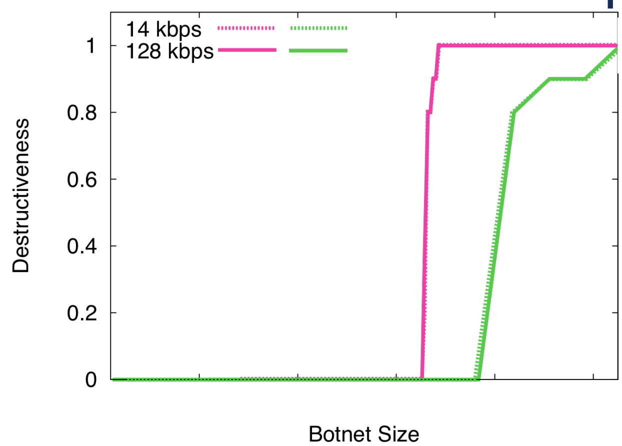
CyLab
www.cylab.cmu.edu
Carnegie Mellon

Destructiveness: 128 kbps



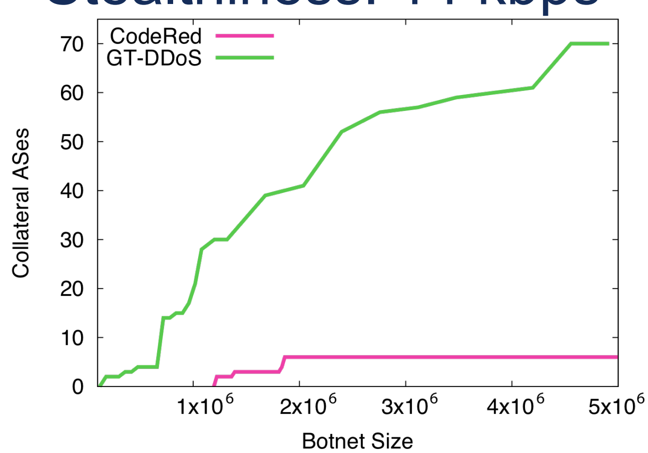
- More bandwidth per attacker requires fewer bots to provide the same destructiveness

Destructiveness: 128 kbps



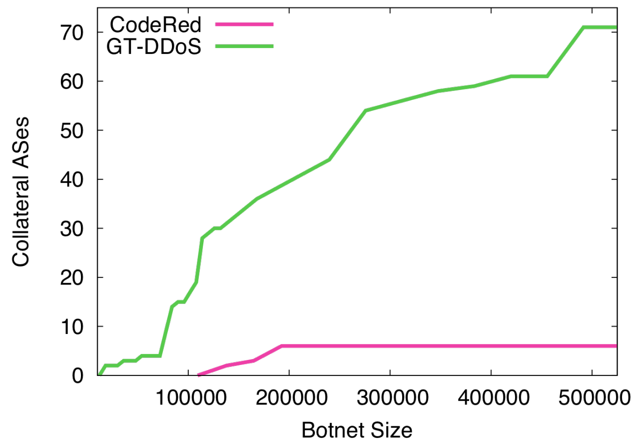
- More bandwidth per attacker requires fewer bots to provide the same destructiveness

Stealthiness: 14 kbps



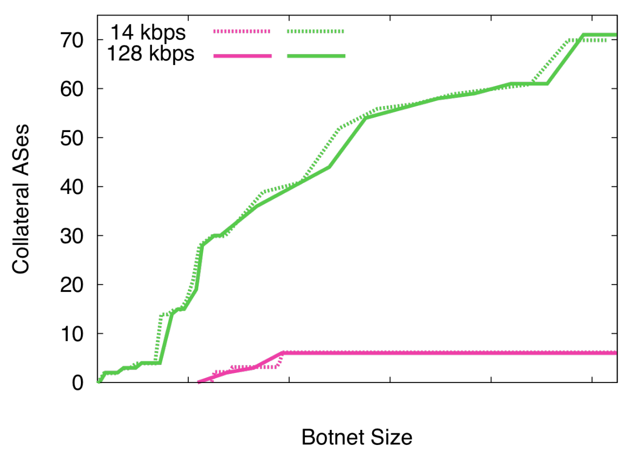
- Greater dispersion causes congestion to fewer collateral ASes

Stealthiness: 128 kbps



- Greater dispersion causes congestion to fewer collateral ASes

Stealthiness



- Bandwidth generation has little impact on the shape of the curves

Simulation vs. Real Attack

- ASes have multiple core links
  - Our topology is a simplification
  - Greater bandwidth available
- Compromised computers have greater resources
- Simulation paths are fixed
  - Facing high loss, paths can change
  - Load balance or shift congestion elsewhere?
- P2P as real life unintentional flooding

Coremelt and DoS Defenses

- Trace back
  - Each bot generates a fraction of the problem
- Capabilities
  - Bots will give each other permissions
- Puzzles
  - Computation becomes the bottleneck
- Fair BW allocation based on src/dst pair
  - Distributed botnet means a fair share ($O(N^{-2})$) is much less than users typically experience

Should we be scared?

- Large enough botnets exist
  - "Storm worm infected millions of hosts"
- What is the motivation?
  - Previously DoS was part of extortion
  - Untargeted attack: disables a portion of the web
  - Extortion on that scale is infeasible
- Cyberwar/terror

Conclusion

- The Coremelt attack presents a new threat to the Internet
- Realistic simulations have shown the attack can succeed
- Requires new defenses to mitigate the threat