Withstanding Multimillion-Node Botnets

Colin Dixon
Arvind Krishnamurthy, Tom Anderson
Affiliates Day, 2007
Botnets

- A botnet is a large group of infected computers controlled by a hacker
- Used to
  - Send spam
  - Steal personal information
  - Launch DDoS attacks
    - Extortion/Protection Rackets
    - Attack rivals
Big Honkin’ Botnet - 1.5 Million!

Published: 2005-10-20
Last Updated: 2005-10-20 21:13:23 UTC
by Ed Skoudis (Version: 1)

A diligent reader from the Netherlands requesting anonymity (lots of folks doing that today) reported on a botnet bust in the Netherlands. The article is in Dutch, but our reader translates it thusly:

"The botnet in the spotlight by the Dutch National Criminal Investigation Unit in the Netherlands comprises approximately 1.5 million hacked computers (instead of 100K reported earlier). The Dutch Computer Emergency Response Team, while dismantling the network of computers infected with spyware, number of infected computers, it was estimated that only 30,000 were located in the Netherlands. The court of Breda has decided to keep the 19-year old suspect as well as a companion, in custody. The suspect is believed to have been responsible for a so-called Denial of Service (DoS) attack after an extortion attempt of a US bank. Investigation both of them were suspected of being involved in another DoS attack of a US bank.

More arrests related to this investigation are anticipated."

Woohoo! Bad guys in jail. You gotta love that.

Vint Cerf: one quarter of all computers part of a botnet

By Nate Anderson | Published: January 25, 2007 - 04:35PM CT

The World Economic Forum takes place this week in Davos, Switzerland, and leaders around the world gather to discuss issues like the Iraq war, global climate change, and globalization—along with the incredible prevalence of botnets.

The BBC's Tim Weber, who was in the audience of an Internet panel featuring Vint Cerf, Michael Dell, John Markoff of the New York Times, and Jon Zittrain of Oxford, came away most impressed by the botnet statistics. Cerf told his listeners that approximately 600 million computers are connected to the Internet, and that 150 million of them might be participants in a botnet—nearly all of them unwilling victims. Weber remarks that "in most cases the owners of these computers have not the slightest idea what their little beige friend in the study is up to."

If Cerf's estimate is accurate, that's one quarter of all machines connected to the Internet. So is the Internet doomed? Well, you're reading this, so no, not yet. But the botnet menace is no phantom, and it has been growing in strength for years. In September 2006, security researcher Symantec.

Computer users typically do not know that their PC has been hijacked.

More than a third of all computer attacks in the second half of 2006 originated from PCs in the United States, the threat report said.

While the total number of bot-net PCs rose, the number of servers controlling them dropped by about 25% to 4,700, the twice-yearly report said.
Botnets are Big

- Total bots:
  - 6 million [Symantec]
  - 150 million [Vint Cerf]
- Single botnets have numbered 1.5 million
- Average upload bandwidth: 3 Mb/s
- Back of the envelope: 4.5-450 Tb/s
  - Flood many core links, small-medium ISPs
How DoS Works
How DoS Works
How DoS Works
Our Approach

- Swarm of machines forward traffic
- Explicitly request each packet
- Attacks must down all mailboxes and thus all paths
Mailboxes

- A large number of machines offer to carry traffic for certain destinations
- Rather than immediately forward it, they buffer traffic until a request is received
- This building block provides two key advantages
  - Filtering logic is left at the destination
  - The system as a whole is fail-stop
The Mailbox

The Mailbox
Many Mailboxes

- Send traffic randomly among mailboxes
Many Mailboxes

- Send traffic randomly among mailboxes
- Botnet can take down one mailbox
Many Mailboxes

- Send traffic randomly among mailboxes
- Botnet can take down one mailbox
- But communication continues
Many Mailboxes

- Send traffic randomly among mailboxes
- Botnet can take down one mailbox
- But communication continues
- Diluted attacks against all mailboxes fail
Attackers can ignore the mailboxes and just attack the server (Filtering Ring)
Remaining Details

- Attackers can ignore the mailboxes and just attack the server (Filtering Ring)
- Before a connection starts, the server has no idea to request packets (General Requests)
Filtering Ring

- Keeps a list of requested packets
- Drops all unrequested packets
- Protects thin access links
- Deployed in depth to counter “insider attacks”
General Requests

- First packets unexpected => can’t request
- Filtering ring prevents unrequested packets from reaching the server
- Solution: Issue some small number of general requests to the mailboxes
  - Allow “first packets” through the filtering ring
  - Provides admission control
  - Limit access by auth tokens & crypto-puzzles
Complete System

- Lookup mailboxes for a server from a distributed name service (CoDoNs)
- Contact one mailbox for a puzzle
- Present a solution and wait
- Mailbox forwards solution to the server
- Server responds and begins to request packets
Key Features

- Unilaterally Deployable
  - Pay Akamai for mailboxes
  - Pay upstream ISP to install filtering ring
- Server is in complete control
  - Explicitly asks for each packet
  - Is not required to trust any given mailbox
- System is fail-stop
DoS Resilience

- Established connection
DoS Resilience

- Established connection
- Attack kills some mailboxes
DoS Resilience

- Established connection
- Attack kills some mailboxes
- “Goodput” decreases
DoS Resilience

- Established connection
- Attack kills some mailboxes
- “Goodput” decreases
- Client sends faster (more redundantly) to compensate
DoS Resilience

![Graph showing packets sent and received over time. The graph indicates a steady increase in packets sent, with fluctuations in the number of packets received. The x-axis represents time in seconds, and the y-axis represents packets per second. The legend indicates two lines: one for 'sent' and another for 'received.' The 'sent' line starts at the lower left and rises gradually towards the upper right. The 'received' line remains stable and is positioned below the 'sent' line.](image-url)
Conclusions

- We have presented a system to mitigate Denial of Service attacks which can be unilaterally deployed today.
- Performance is reasonable with few optimizations, still room for improvement.
- Can scale to deal with the massive botnets of today and tomorrow.
Questions?