



# Evaluating Attack Amplification in Online Social Networks

**Blase E. Ur and Vinod Ganapathy**

**[blaseur@rci.rutgers.edu](mailto:blaseur@rci.rutgers.edu) , [vinodg@cs.rutgers.edu](mailto:vinodg@cs.rutgers.edu)**

**Rutgers University**

# Online Social Networks

- **facebook**

- 200 million monthly unique visitors
- Founded in 2004



- 

- 126 million monthly unique visitors
- Founded in 2003

- **flickr™**

- 64 million monthly unique visitors
- Founded in 2004

# Hubs Exist in Social Networks

- Hubs- very popular users
  - Large number of friends
  - Large number of page views
- Average MySpace user has 200 friends
- MySpace Hubs include celebrities, musicians
  - Rihanna: 1,600,000 friends, 85,000,000 views
  - Tila Tequila: 3,700,000 friends, 184,000,000 views

# Hubs Enable Attack Amplification

- Attack Amplification: increasing the effects of an attack by coercing a large number of Web users to unwittingly join in
- Hubs are treated the same as ordinary users
- By posting on hubs' pages, ordinary users can amplify attacks
- This threat should be stopped by Social Networks

# Outline

- Motivation
- Background on Social Networks
- Attack Description
- Evaluation
- Remediation

# Anatomy of a MySpace Page

myspace.com  
a place for friends.

Music Search POWERED BY Google

Home Browse People Find Friends Local Music Video More Titus Andr.. Log In Sign Up

myspace
music
my music | music videos | featured playlists | top artists | shows | classifieds | forums

## Titus Andronicus

Indie / Punk / Shoegaze

The enemy is everywhere.



GLEN ROCK, NEW JERSEY  
United States

Profile Views:  
517173

Last Login:  
5/8/2009

View My: [Pics](#) | [Videos](#) | [Playlists](#)

myspace music
Pop Out Player



⏮
⏪
⏸
⏩
⏭

**Titus Andronicus**  
Titus Andronicus

00:41 

 03:16

📱 Ringtones Add Buy

- ▶ **Titus Andronicus** by Titus Andronicus
192,390 plays
+
- Landscape with Icarus** by Titus Andronicus
109,563 plays
+
- Titus Andronicus Forever** by Titus Andronicus
25,826 plays
+
- Every Time I See the Light pt1** by Titus Andronicus
20,716 plays
+
- Joset of Nazareth's Blues** by Titus Andronicus
36,366 plays
+

Albums (0)
Statistics
Playlists (0)

Contacting Titus Andronicus

- ✉ Send Message
- 👤 Add to Friends
- 📞 IM / Call
- 👥 Add to Group

- ✉ Forward to Friend
- 📁 Add to Favorites
- 🚫 Block User
- 🏆 Rank User

MySpace URL:  
[www.myspace.com/titusandronicus](http://www.myspace.com/titusandronicus)

Titus Andronicus: General Info

Member Since	5/30/2005
Dead Website	<a href="http://www.titusandronicus.net">www.titusandronicus.net</a>

Upcoming Shows (view all)

May 14 2009	8:00P	<b>The Volks Great Escape</b>	Brighton
May 15 2009	8:00P	<b>Water Margin Great Escape w/ The Soft Pack</b>	Brighton
May 16 2009	8:00P	<b>Lennons</b>	SOUTHAMPTON
May 18 2009	8:00P	<b>Academy w/ the Soft Pack</b>	Oxford
May 19 2009	8:00P	<b>Academy 3 w/ the Soft Pack</b>	Birmingham
May 20 2009	1:15P	<b>Instore @Pure Groove</b>	London, London and South East

# Comments Allow HTML

<p><b>CAPTAIN POLAROID and the Betamax Conspiracy</b></p> 	<p><b>May 9 2009 6:28 AM</b></p> <p>Grr I was gonna come see you in Birmingham UK but I'm already going to gig that day! Typical! Please come back again...</p>
<p><b>Industry Open mic Now Broadcasts live on 90.3FM!!</b></p> 	<p><b>May 8 2009 9:48 AM</b></p> <p>HI!,WE WOULD LIKE TO INVITE TO OUR OPEN MIC RADIO SHOWCASE THIS TUESDAY! AND EVERY TUESDAY!</p> <p>THE LAST SHOW WAS THE LAUNCH AND WAS HUGE!!!</p> <p>OUR OPEN MIC WAS BROADCASTED ON 90.3FM!!!!</p> <p>AND WILL BE AIRING NOW EVERY WEEK!</p> <p>PERFORMERS CAN LISTEN TO THEIR PERFORMANCE THE VERY NEXT DAY ON 90.3FM WITH FRIENDS AND FAMILY!</p> <p>THIS IS MAJOR EXPOSURE! 700,000+ LISTENERS!</p> <p>THIS TUESDAY @ THE KARMA LOUNGE FIRST AVE BETWENE 3RD AND 4TH STREET MANHATTN NY</p> <p>ARTIST SIGN UP 8.30PM</p> <p>SHOW STARTS 9.30PM</p> <p>ADMISSION ONLY \$10</p> <p>HOPE YOU CAN MAKE IT!</p> 

HTML

# Outline

- Motivation
- Background on Social Networks
- Attack Description
  - Denial of Service
  - Botnet Command & Control
- Evaluation
- Remediation



# DoS Attack

## Hub's Page



# DoS Attack

Hub

Jon

Dec 5 11:47 AM

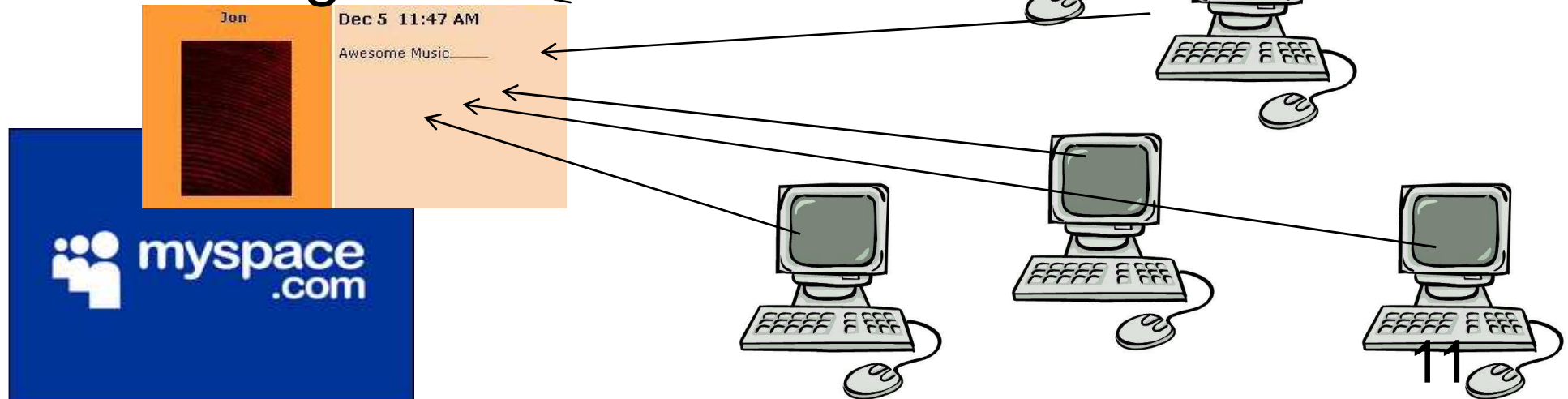
Awesome Music \_\_\_\_\_



# DoS Attack

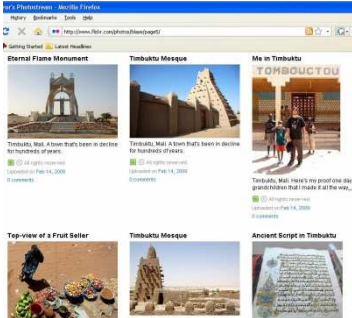
Internet Users

Hub's Page

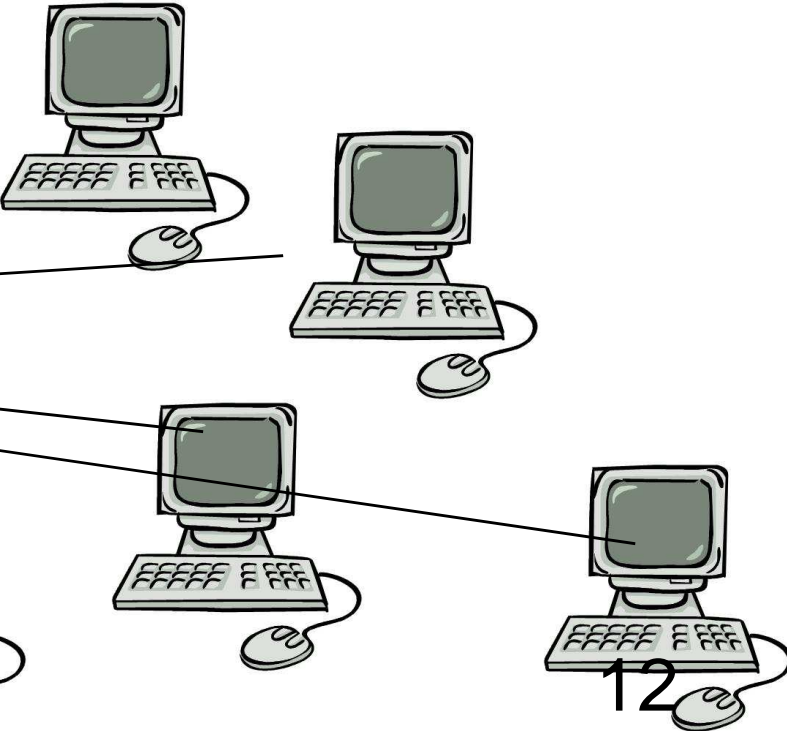


# DoS Attack

## Victim Web Server



## Internet Users



## Hub's Page

A Myspace.com logo is shown in a blue box. To its right is a snippet of a user profile for 'Jen', dated 'Dec 5 11:47 AM', with the text 'Awesome Music'. Arrows from the 'Internet Users' point to this profile snippet.

# DoS Attack

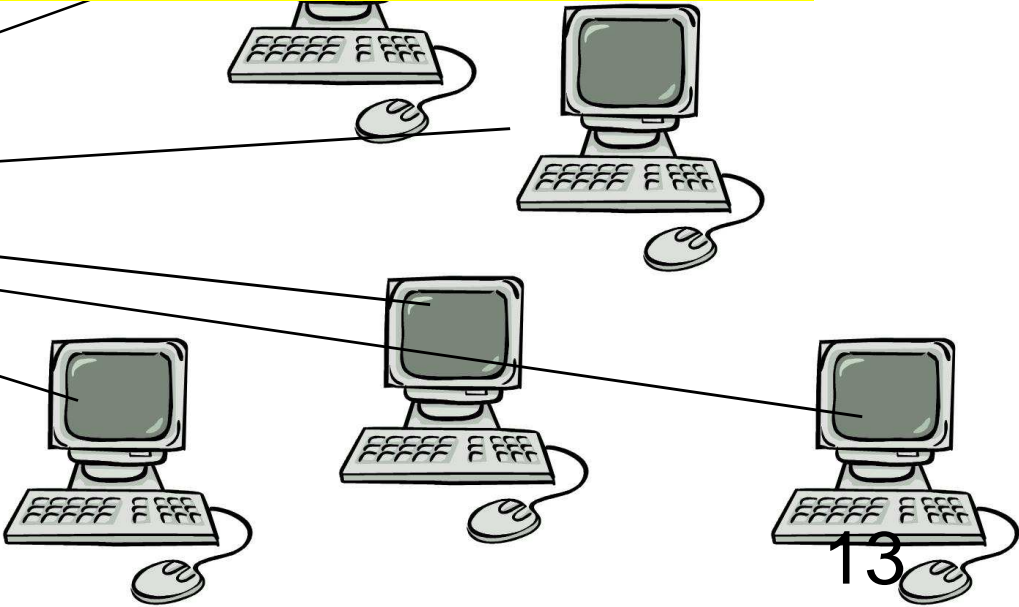
Victim Web Server



Can be launched by an arbitrary Web user

s

Hub's Page



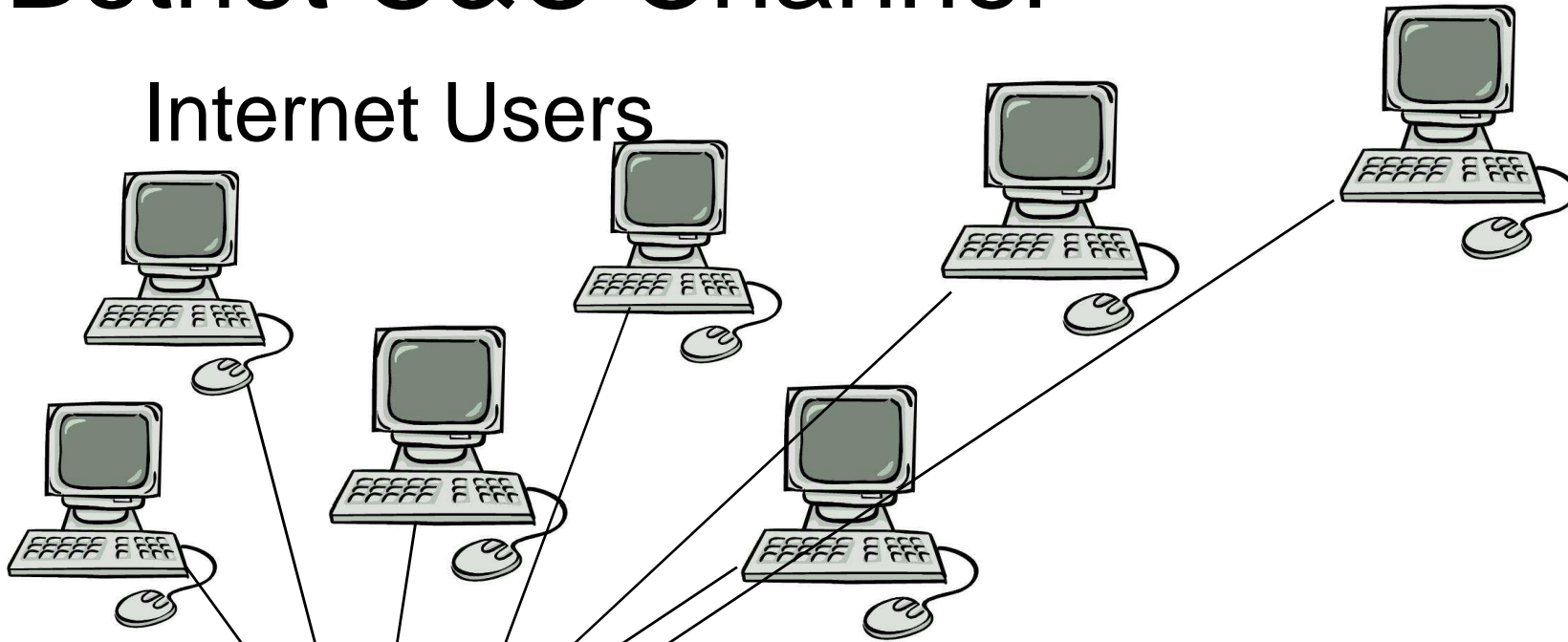
# Botnet C&C Channel

## Hub's Page



# Botnet C&C Channel

Internet Users

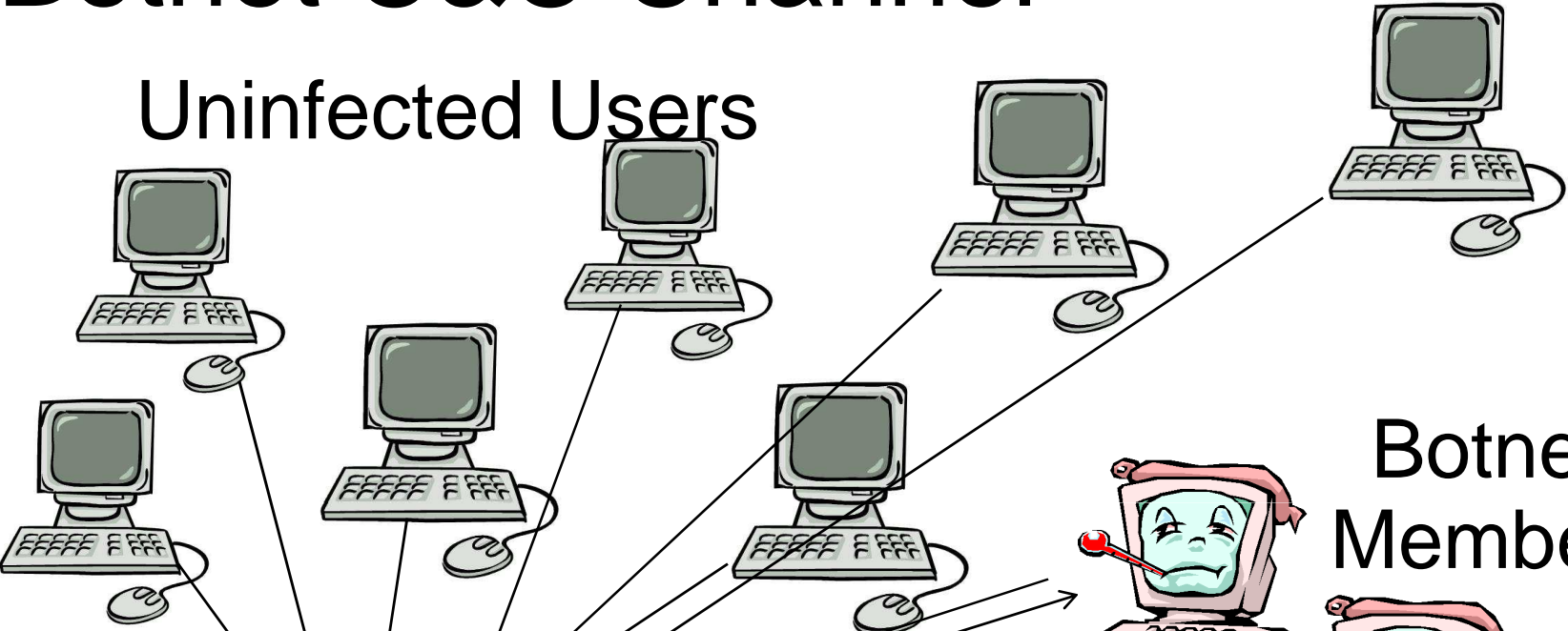


Hub's Page



# Botnet C&C Channel

Uninfected Users



Botnet Members

Hub's Page





# Outline

- Motivation
- Background on Social Networks
- Attack Description
- Evaluation
- Remediation

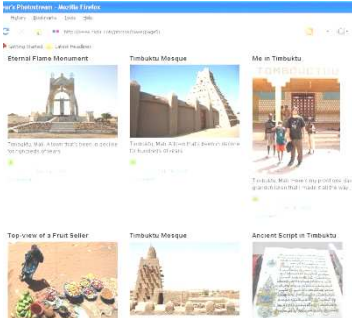
# Methodology

Today's Top Artists			
	Unsigned	Indie	Major
1	 <b>Never Shout Never</b> (another n... Joplin Lounge	 <b>3OH!3 (is on the 2009 AP TOUR)</b> BOULDER, Colorado Rock / Electronica / Thrash	 <b>Beyonce</b> NEW YORK, New York R&B / Hip Hop / Pop
2	 <b>Arcangel</b>	 <b>paramore</b> Franklin, Tennessee Alternative / Pop / Regional Mexican	 <b>Taylor Swift</b> Nashville, Tennessee Country / Acoustic / Folk
3	 <b>Pitbull</b> MIAMI, Florida Hip Hop	 <b>The Devil Wears Prada (NEW ...)</b> Dayton, Ohio Hardcore / Metal / Christian	 <b>Akon</b> Atlanta, Georgia Hip Hop / R&B / Pop

- Post comments on MySpace hubs' profiles
- Comments hotlink images from own server
- 1,073 out of 3,000 permitted HTML
- 942 out of 1,073 accepted friend request

# DoS Research Questions

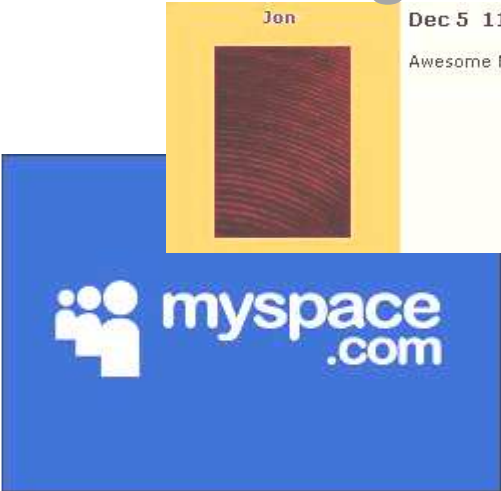
Victim Web Server



Internet Users



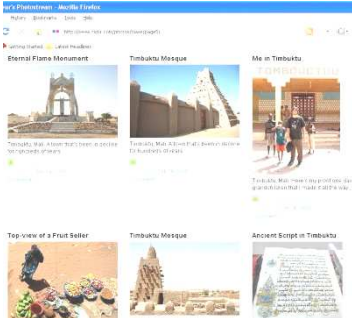
Hub's Page



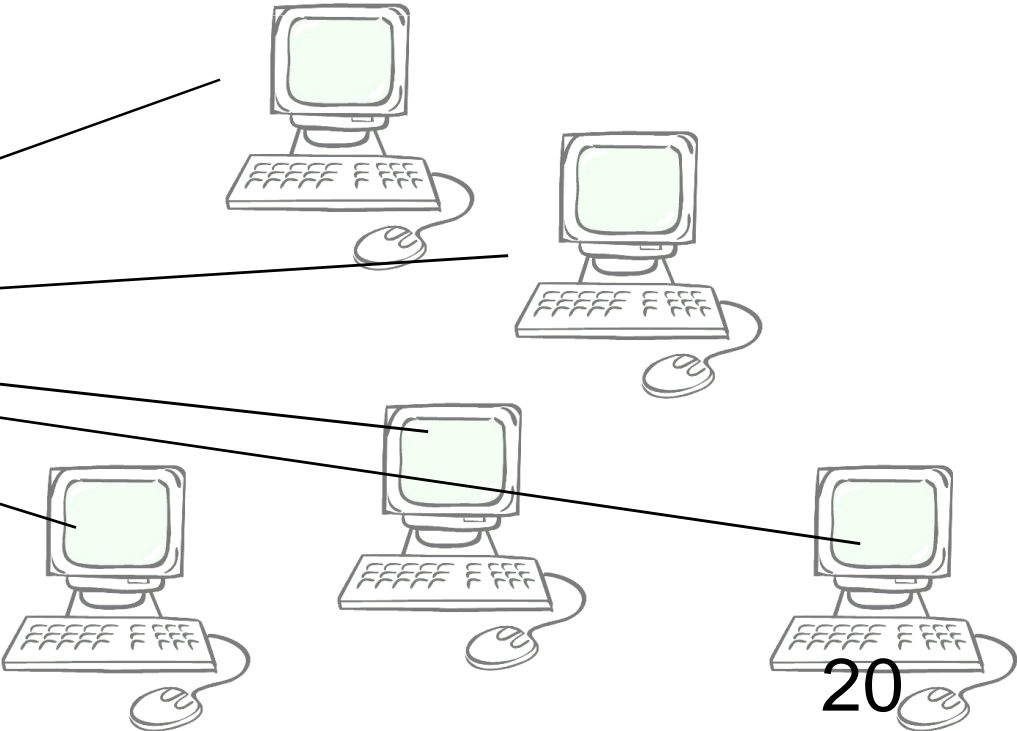
1. How many internet users join the attack?

# DoS Research Questions

Victim Web Server



Internet Users



Hub's Page

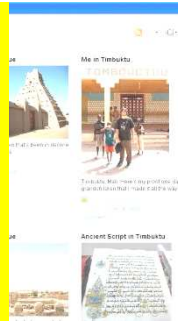


2. How do hubs differ in popularity?

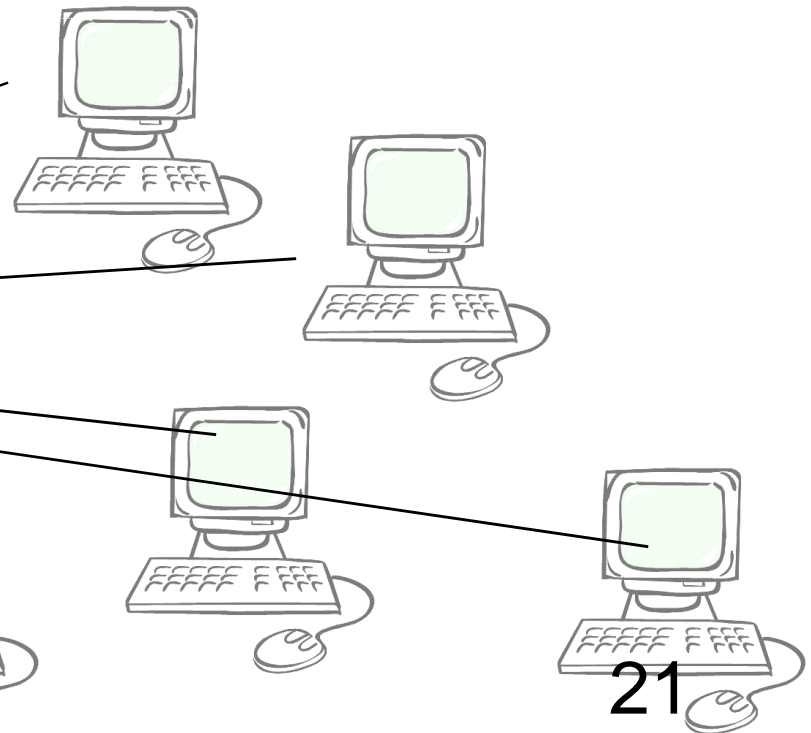
# DoS Research Questions

Victim Web Server

3. How much bandwidth does each user direct to the victim?



Internet Users



Hub's Page

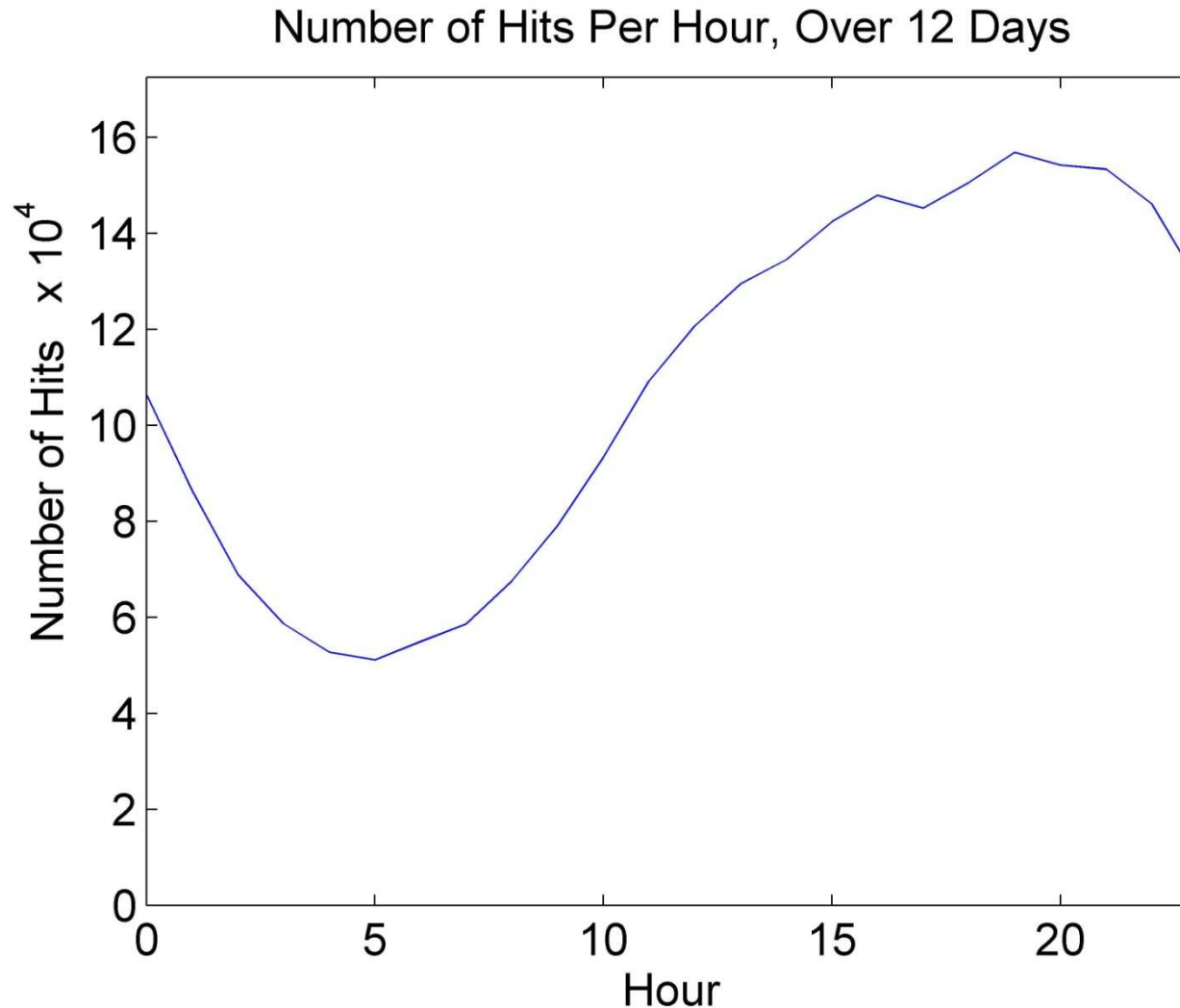


# DoS- How Many Users

- **Goal:** How many users will take part?
- **Method:** Hotlink 1 pixel image, 12 days
- 719 different profiles
- 2,598,692 total hits
- 1,828,589 unique IP addresses



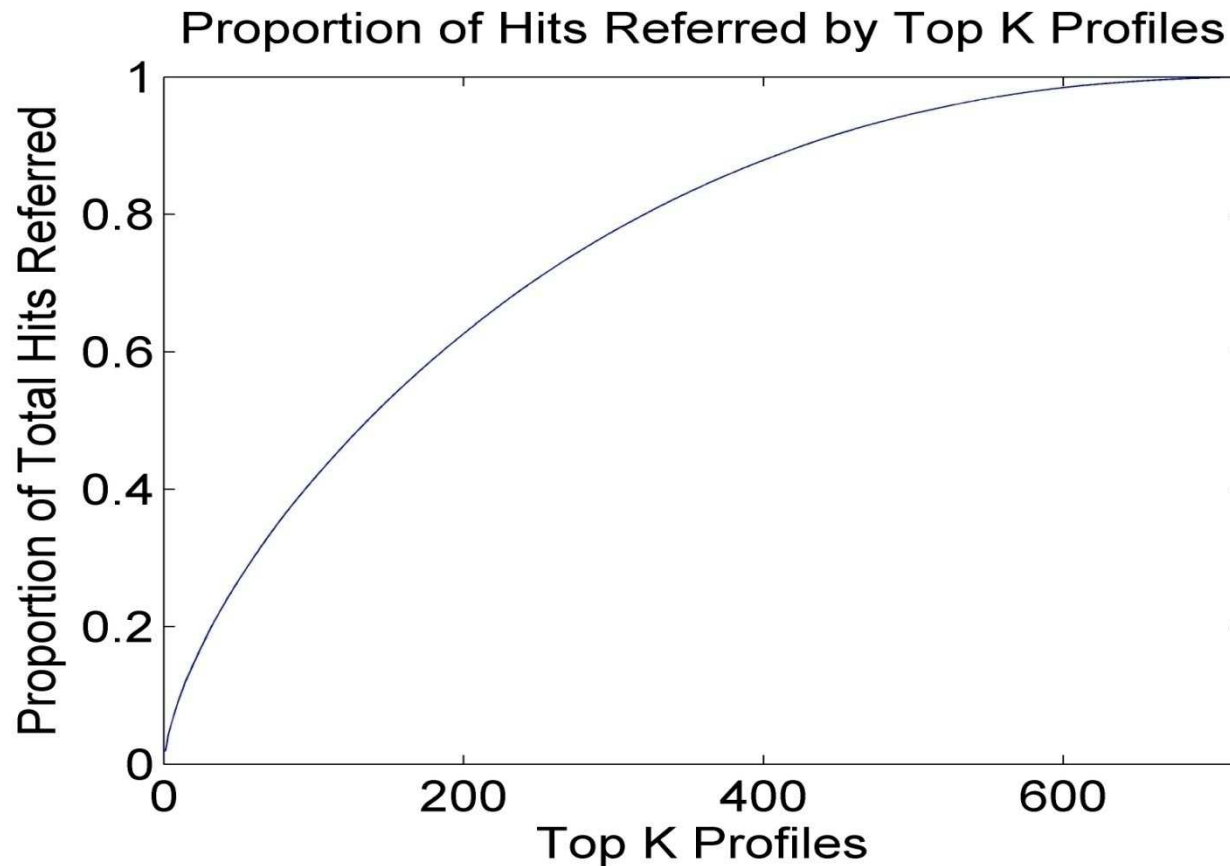
# DoS- Diurnal Patterns



- A very large number of users participate

# DoS- Hub Popularity

- **Goal:** How do hubs differ in popularity?



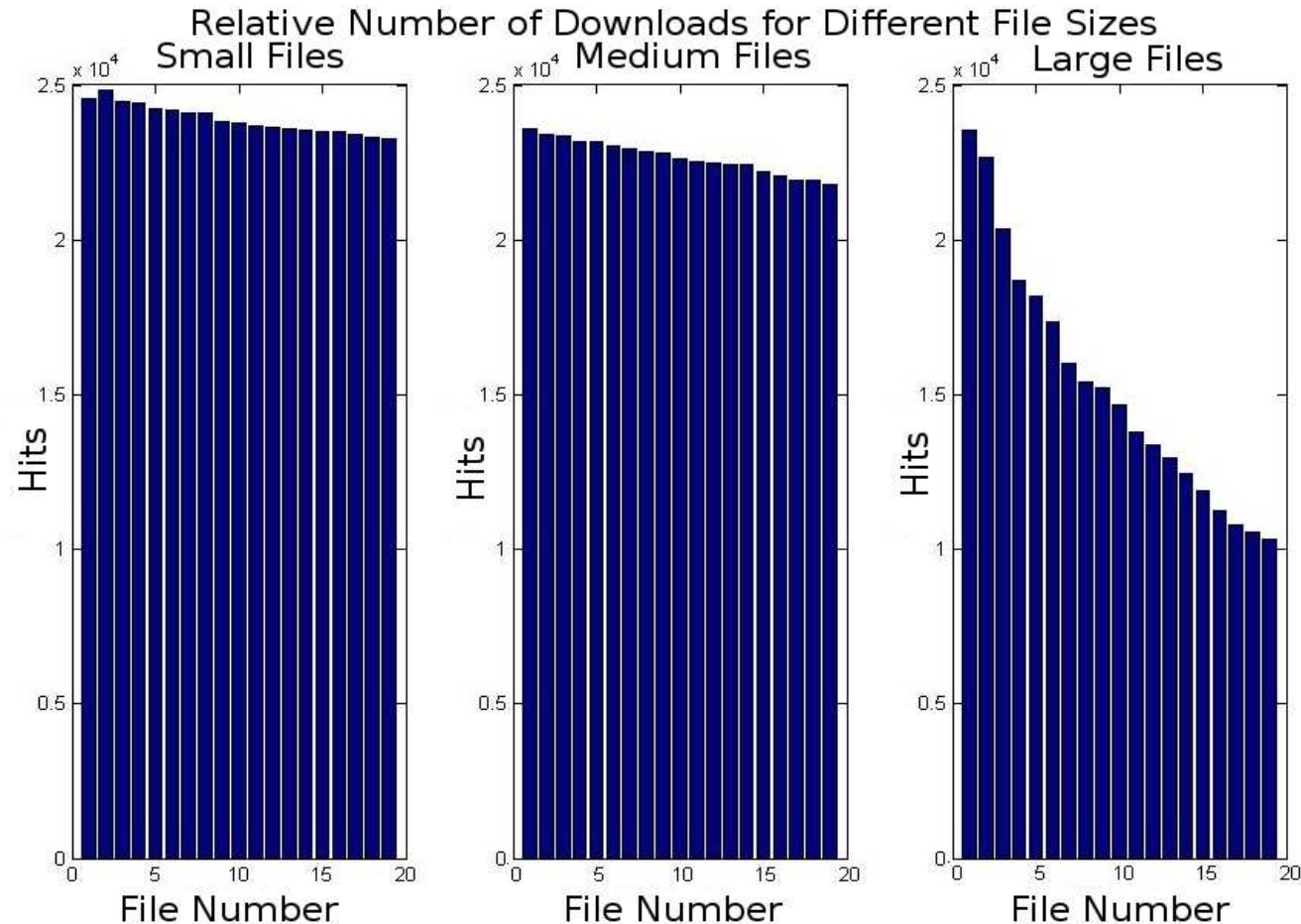
- 1% of the hubs provide 10% of the traffic



# DoS- Total Bandwidth

- **Goal:** Are users leaving pages and reducing the bandwidth directed to a victim server?
- Total size of all files in comment: 42 MB
- **Method:** Hotlink 19 small (20 kb), 19 medium (80 kb), 19 large (2 MB) images

# DoS- Total Bandwidth

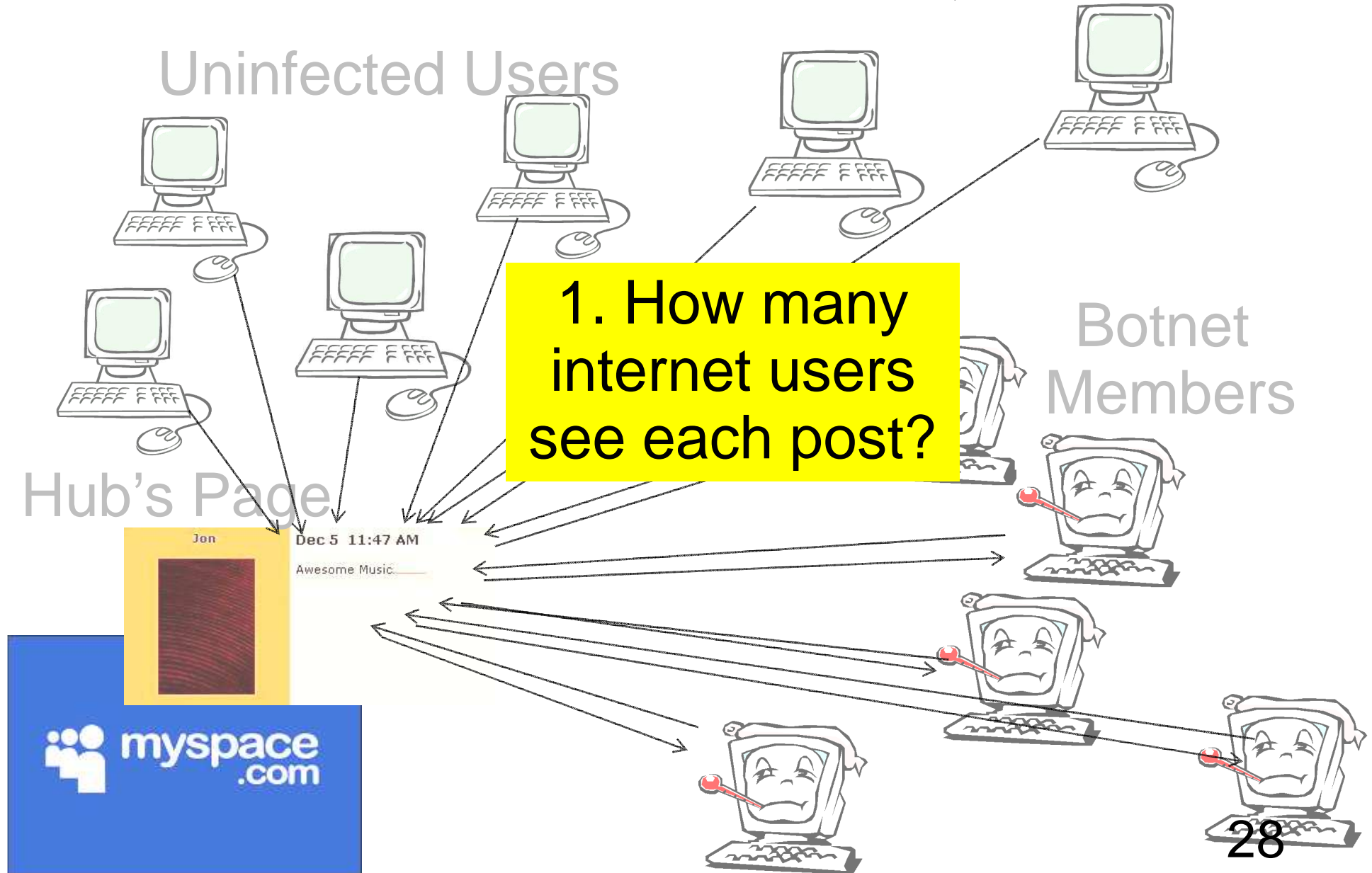


- Users are leaving pages before they load
  - 60% of theoretical efficiency (42 MB)

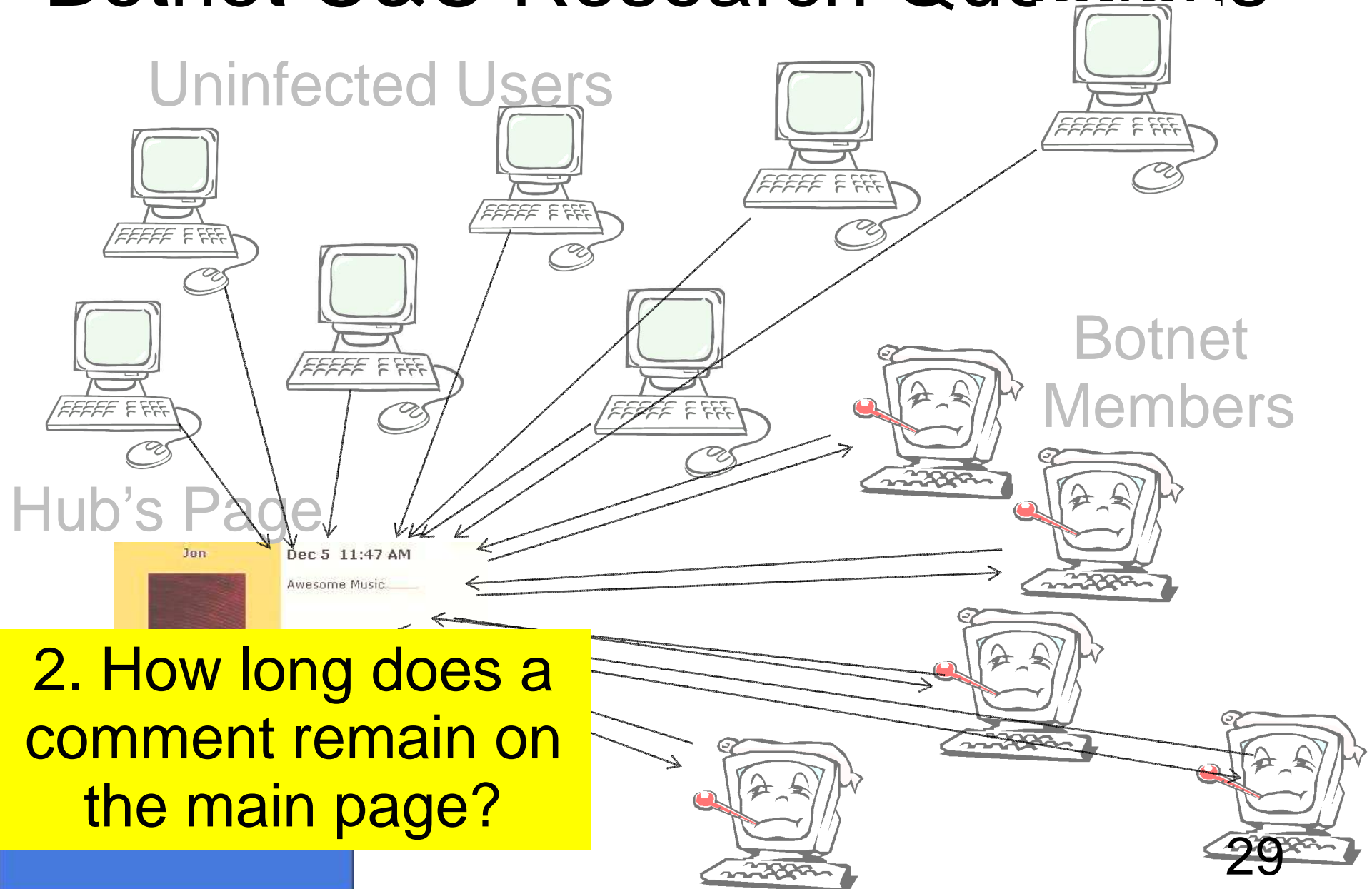
# DoS- Total Estimate

- Hotlink 42 MB on 719 profiles
- 65 Terabytes total (12 days)
- 525 Gigabytes directed toward victim server in the peak hour
  
- Attackers Can Concentrate on Top 10 Hubs
- Hotlink 42 MB on top 10 profiles
- 6.5 Terabytes total (12 days)
- 52.5 Gigabytes directed toward victim server in the peak hour

# Botnet C&C Research Questions



# Botnet C&C Research Questions



# C&C- Lifetime of a Comment

- **Goal:** How long does a comment stay on a page? (Avoid reposting)
- **Method:** Measure when traffic drops below 10% of maximum from each profile
- Median Lifetime of a comment: 137 hours (5.5 days)
- 10 posts can reach 180,000 unique IP addresses over a few days

# Outline

- Motivation
- Background on Social Networks
- Attack Description
- Evaluation
- Remediation

# Technique 1- Restrict Hubs

- By default, disallow HTML/media in posts on popular pages
- Why not restrict all HTML use?
  - Freedom / Customization
  - It's in use and popular
- At what threshold of friends / page views does a user become a hub?



# Technique 2- Focused Monitoring

- Amplification attacks require hubs
- Monitor hubs only for suspicious posts

# Technique 3- Friend Hierarchy

- Only allow friends of a certain relationship (other musicians) or particular social circle to post
- Friend Lists don't suffice
  - Huge time investment, few obvious rewards
  - Requires an automated solution

# Technique 4- Reputation System

- Only allow posts from users whose previous comments have met some criteria
- Require greater time investment from attacker
- What metrics?
- Can be gamed!

# Take-Away Points

- Hubs allow ***arbitrary*** adversaries to ***amplify*** bandwidth-based attacks and the distribution of content
- Just 10 posts by arbitrary user:
  - Reach 180,000 unique IP addresses
  - Can direct 50+ GB of traffic toward a victim server in an hour
- Remediation is necessary at social network
  - Without losing “openness” of network

**Thank You!**

**Evaluating Attack Amplification  
in Online Social Networks**

**Blase E. Ur and Vinod Ganapathy**

**blaseur@rci.rutgers.edu , vinodg@cs.rutgers.edu**

**Rutgers University**