M3AAWG
MESSAGING MALWARE MOBILE

DNS Changer Remediation Study

The following study was presented by
Georgia Tech researchers at the
M3AAWG 27th General Meeting
February 19, 2013, San Francisco

DNS Changer Remediation Study

Wei Meng, Ruian Duan, Wenke Lee

Outline

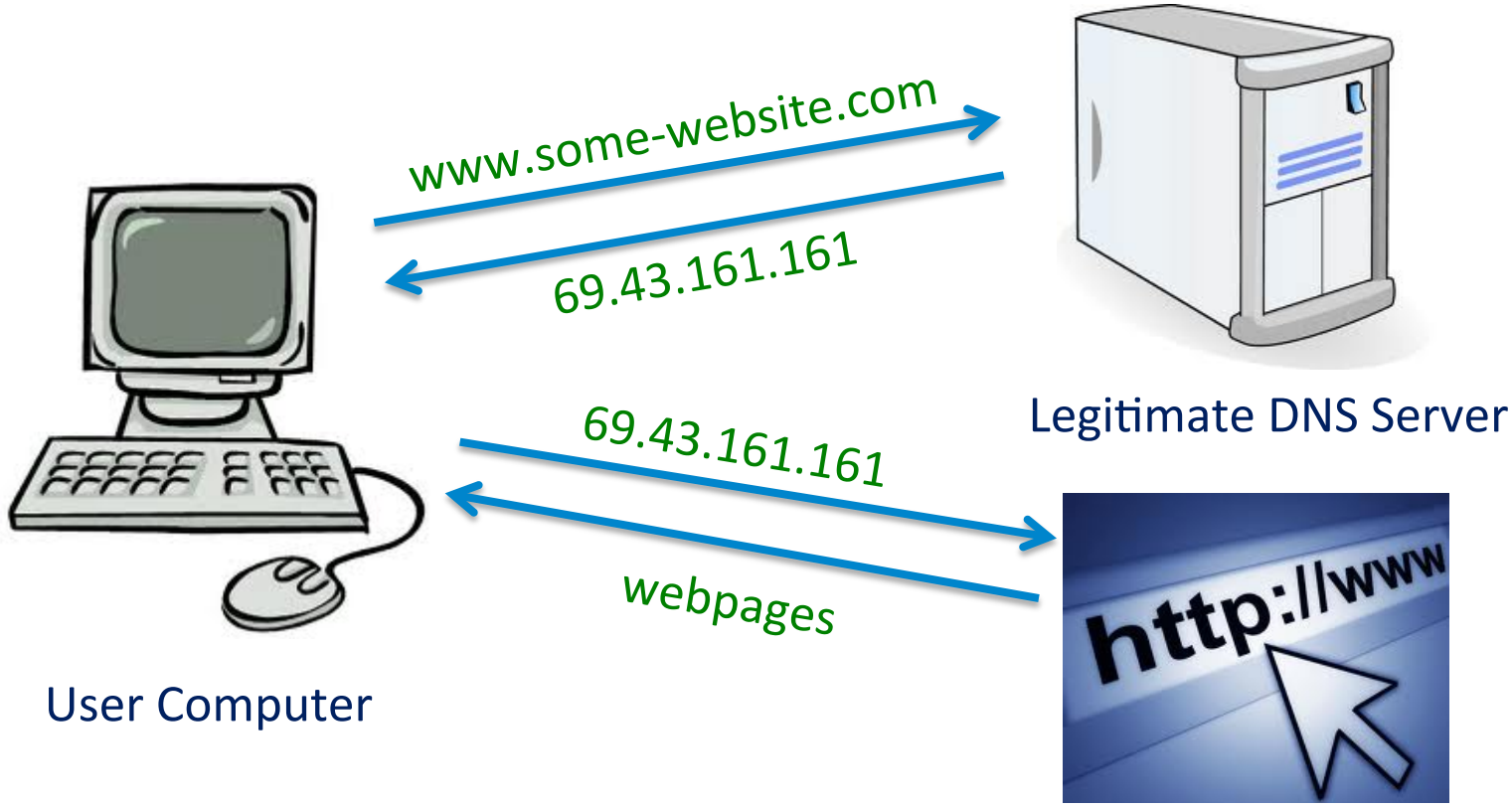
1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. Remediation Strategies for ISPs
6. Recommendation

Outline

1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. Remediation Strategies for ISPs
6. Recommendation

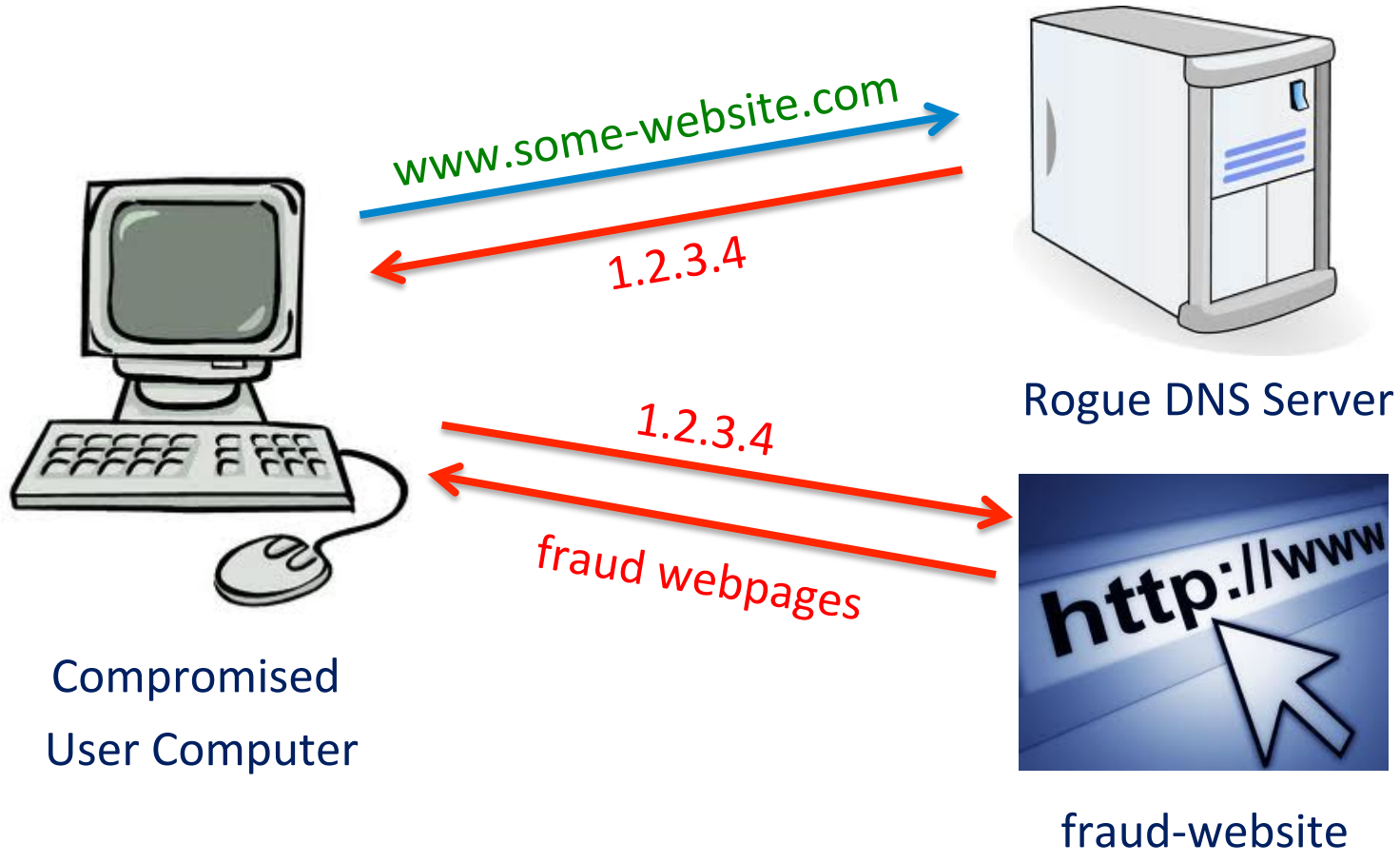
1. Background & Motivation

- Domain Name Service (DNS)
  - One of the most important Internet services



1. Background & Motivation

- DNSChanger
  - A DNS Trojan



1. Background & Motivation

- Why would the bad guys want to redirect victims to rogue DNS servers?
  - $ 14 million!
- Who were infected?
  - Windows and Mac OS X users
  - Networking devices!
- How many users were infected?
  - Over 4 million at its peak

1. Background & Motivation

- FBI's Operation Ghost Click
  - 6 Estonian nationals were arrested
  - Rogue DNS servers operated by Rove Digital were taken over by FBI
  - Court order
    - BIND software of Internet Systems Consortium (ISC) was used to maintain the "clean" DNS server
- Are we OK then?
  - Users may still be infected with other malware
  - ISC maintained DNS servers would be turned off on July 9, 2012!
    - No Internet (WWW, e-mail, VoIP, IM…)

1. Background & Motivation

- Internet Systems Consortium
  - Serving DNS requests from victims
  - Collecting information on the ones still infected
- Internet Service Providers
  - Notifying their customers about infections
  - Providing temporary DNS services
  - Providing support for remediation
- Media & Social Networks
  - Informational and situational awareness campaigns
  - Google, May 22, 2012
  - Facebook, July 6, 2012

1. Background & Motivation

- Our goals
  - Study which remediation strategies were most effective
  - Gain insights into the influence that social networks and online media had on remediation efforts
  - Provide suggestions for countering future threats, effective best remediation practices for ISPs

Outline

1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. Remediation Strategies for ISPs
6. Recommendation

2. Data & Methodology

- DNSChanger infection data
  - Shared by ISC
  - DNS requests to the rogue DNS server controlled by FBI & ISC
  - Nov 8, 2011 – July 10, 2012
  - Format:
    - date, timestamp, src_ip:port, dst_ip:port, TXID, RD flag

2. Data & Methodology

- DNSChanger infection data
  - Every 15 mins, 300-600 MB per file
  - 96 csv files per day
  - Some files were missing (or corrupted …)
  - Data on several days were poisoned due to attacks
  - Data from 35 out of 243 (14.4%) days was dropped

  - Used various GeoIP and IP-to-ASN databases to translate IP addresses to corresponding ISP and country
  - Analysis was conducted on ISP and country code level

2. Data & Methodology

- Online Media – Google Search & Google News
  - Crawled Google Search results using the terms "DNSChanger" and "DNS Changer"
  - Recorded the "post date" of each result
  - Gathered website rank and reputation information from *Alexa.com*
  - Online Media Score:
    - summation of log(website reputation) for all websites

2. Data & Methodology

- Social Network – Twitter
  - Crawled tweets related to “DNSChanger” from November 2011 to February 2013
    - Daily tweet count
    - Post count of each tweet
  - Fetched the profiles of Twitter users who initiated the corresponding tweets
  - Used the log of the number of followers of each user as the influential weight of corresponding tweets
  - Calculated the Twitter Topic Score of each day
    - summation of post count of each tweet multiplied by corresponding influential weight
    - represent how hot the topic was

2. Data & Methodology

- ISP strategies
  - Created one survey server for ISPs to submit data around their remediation actions
  - All submitted data are confidential

2. Data & Methodology

- ISP remediation strategies

1. How and when did you notify the victims of DNS Changer?

Methods	start time(mm/dd/yyyy)	end time(mm/dd/yyyy)	portion of customers reached
☐ Email			Select portion
☐ Billing			Select portion
☐ Phone			Select portion

2. What remediation strategies were used for the DNS Changer botnet?

Strategies	start time(mm/dd/yyyy)	end time(mm/dd/yyyy)	portion of customers reached
☐ Anti-virus software			Select portion
☐ Custom remediation			Select portion
☐ MSRT			Select portion
☐ Enhance firewall			Select portion

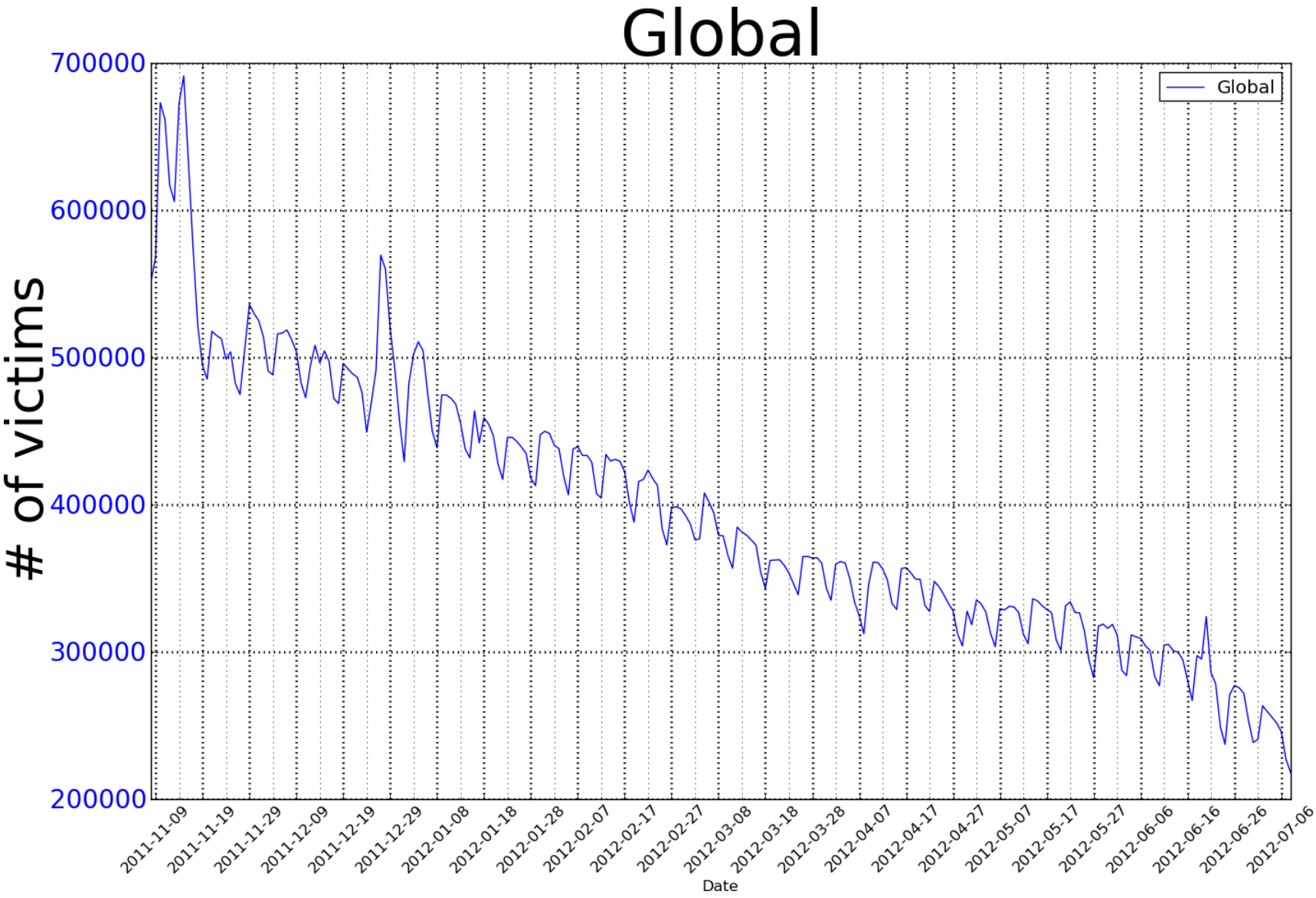
2. Data & Methodology

- Metrics
  - Mitigation Rate
    - the ratio of (moving average of last several days' victim counts) to (maximum victim count)
  - Confidence Score for ISP Strategy
    - Measuring the effectiveness of strategies
    - One-time strategy confidence score:
      - describes how large the victim count decrease rate is within a time window (e.g. 10 days) since the strategy took place
    - Period strategy confidence score:
      - describes how large the victim count decrease rate is within the period that a strategy was active

Outline

1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. Remediation Strategies for ISPs
6. Recommendation

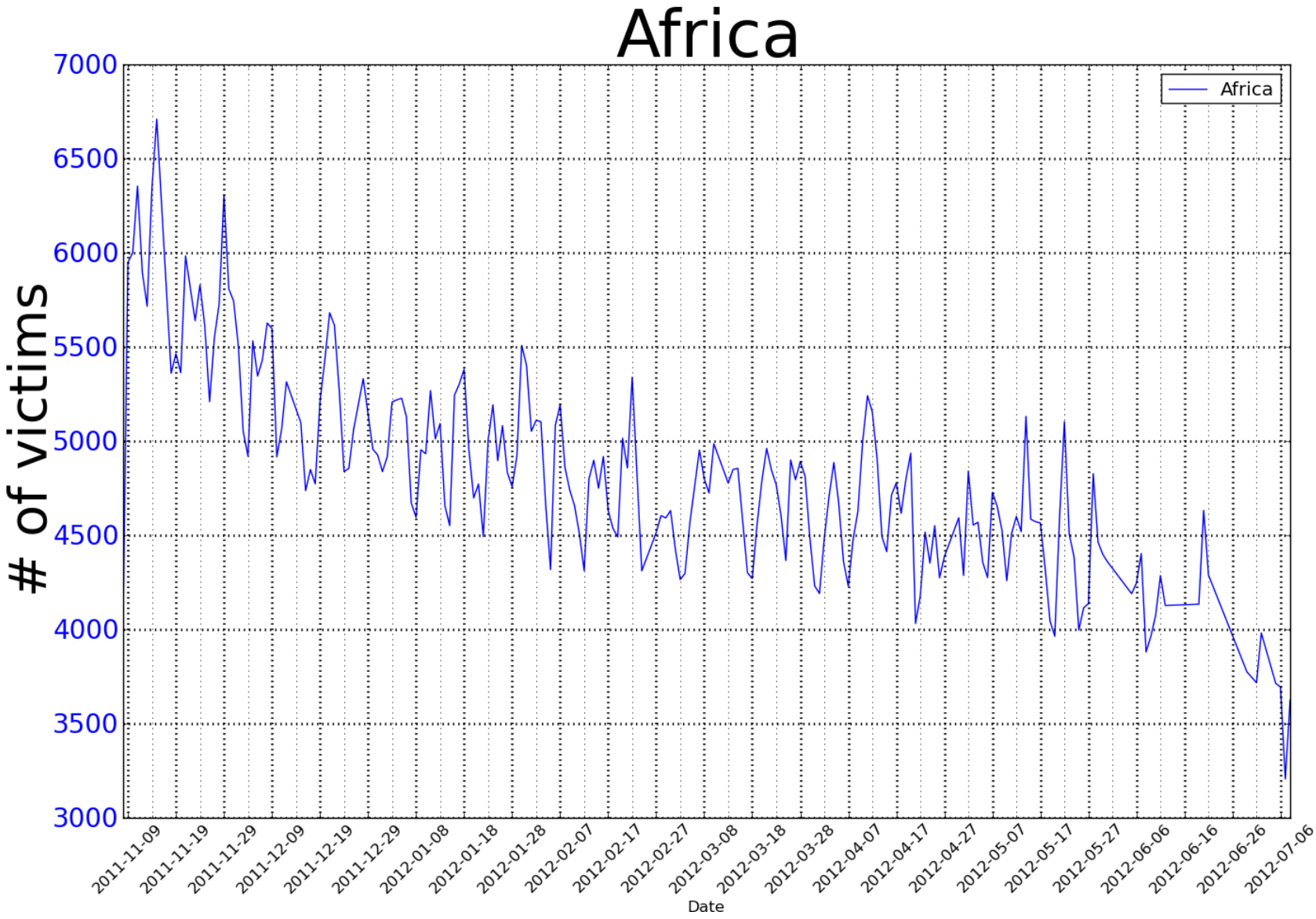
3. Statistics



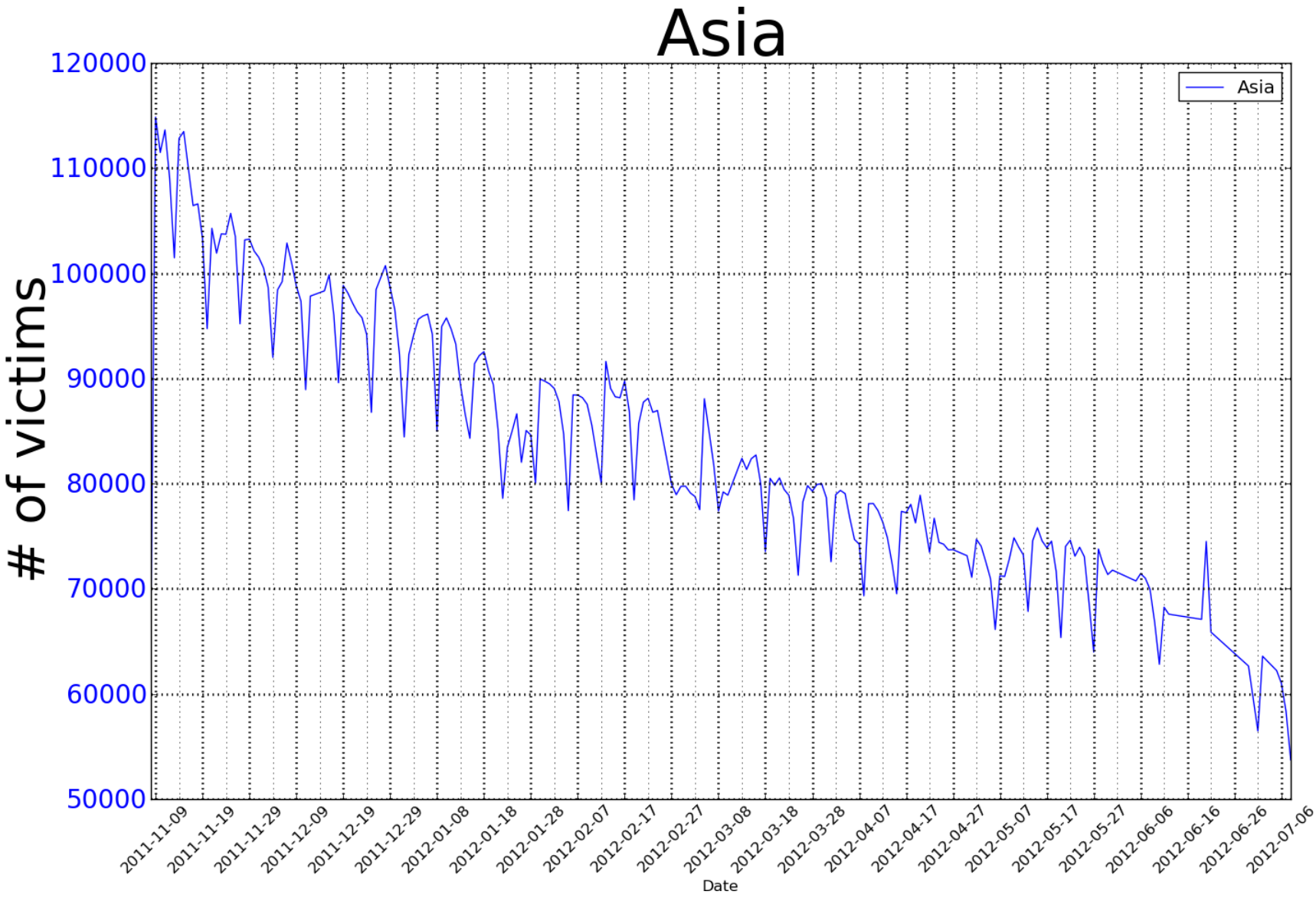
3. Statistics

- Infections per continent (daily count)

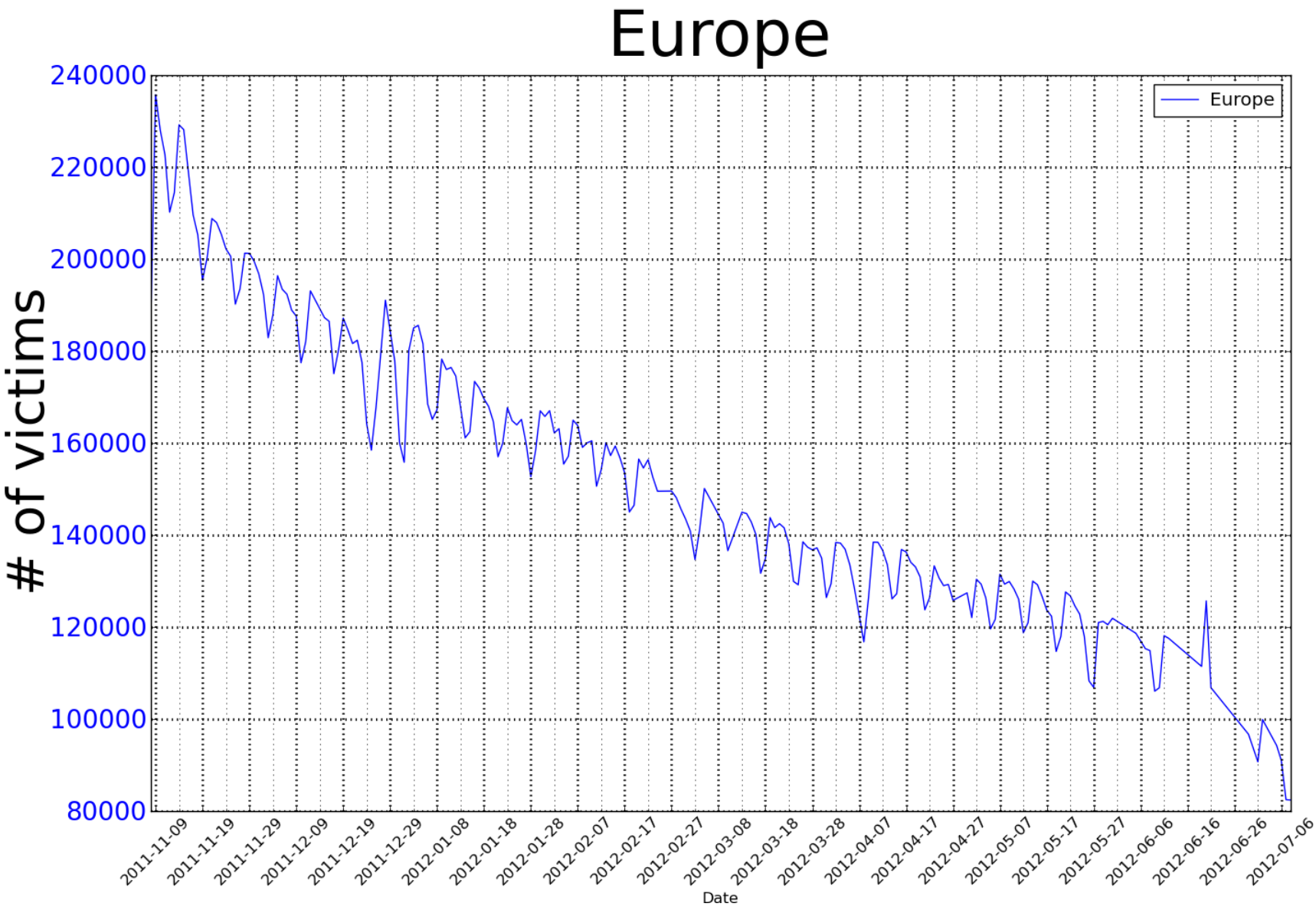
3. Statistics



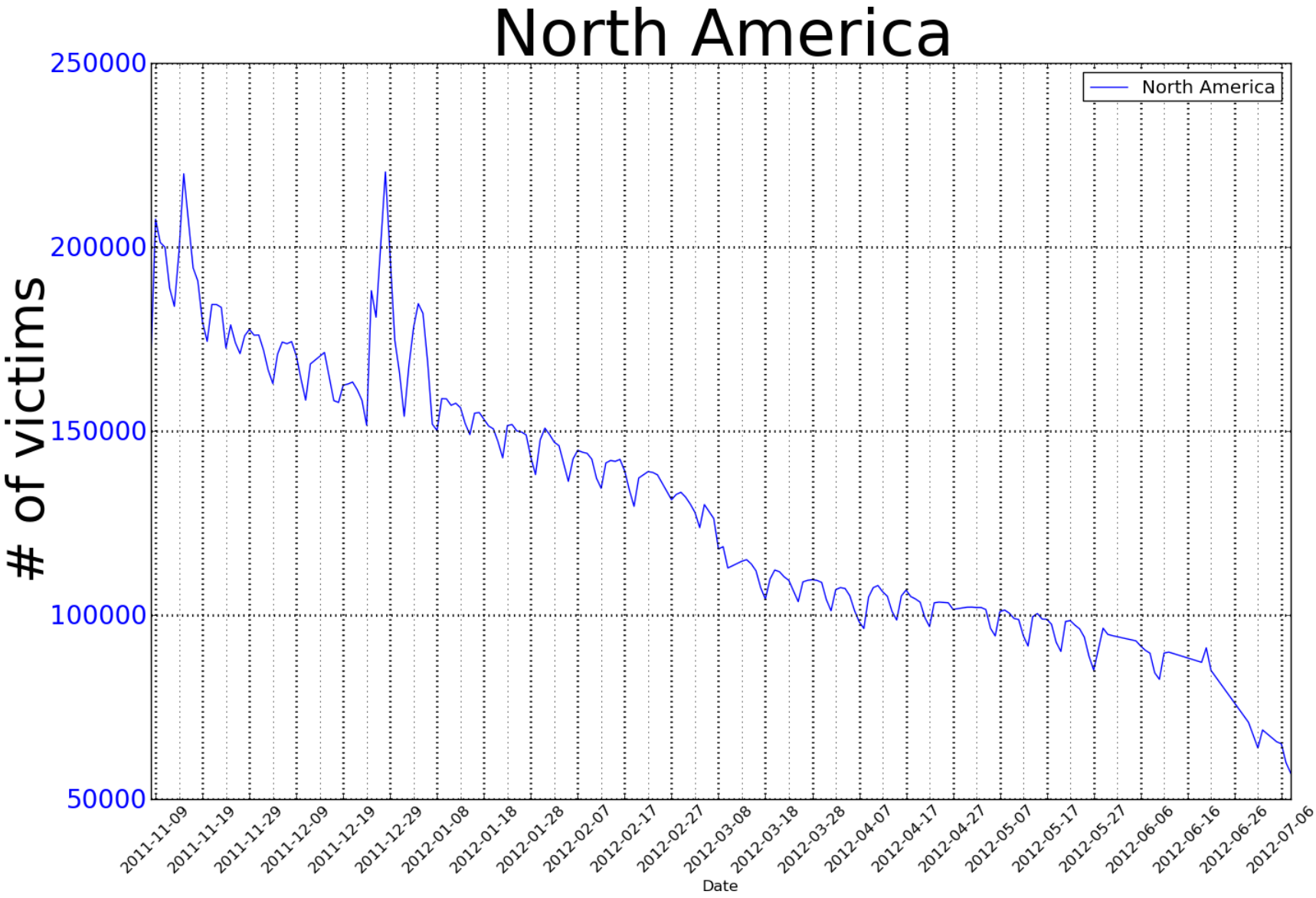
3. Statistics



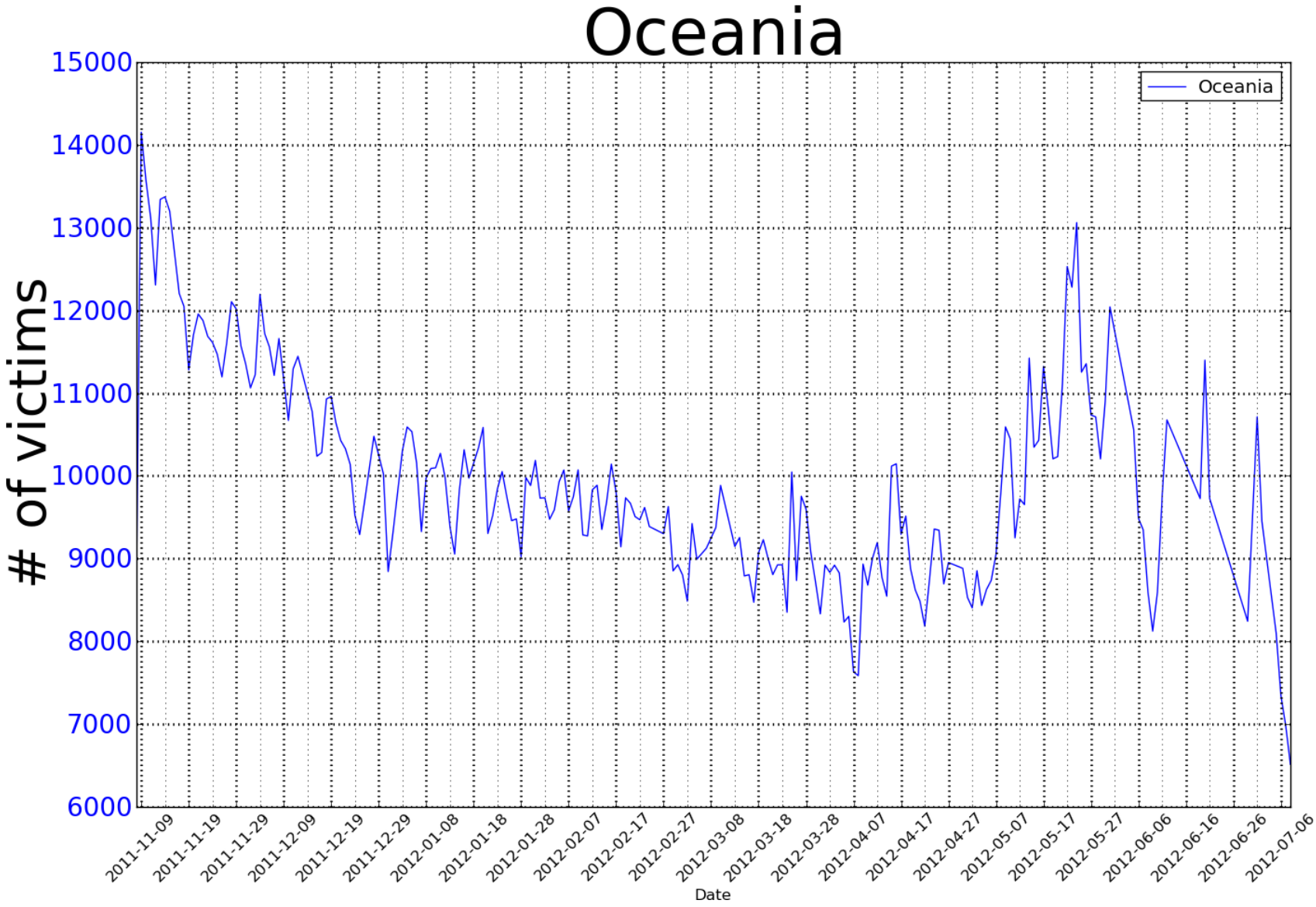
3. Statistics



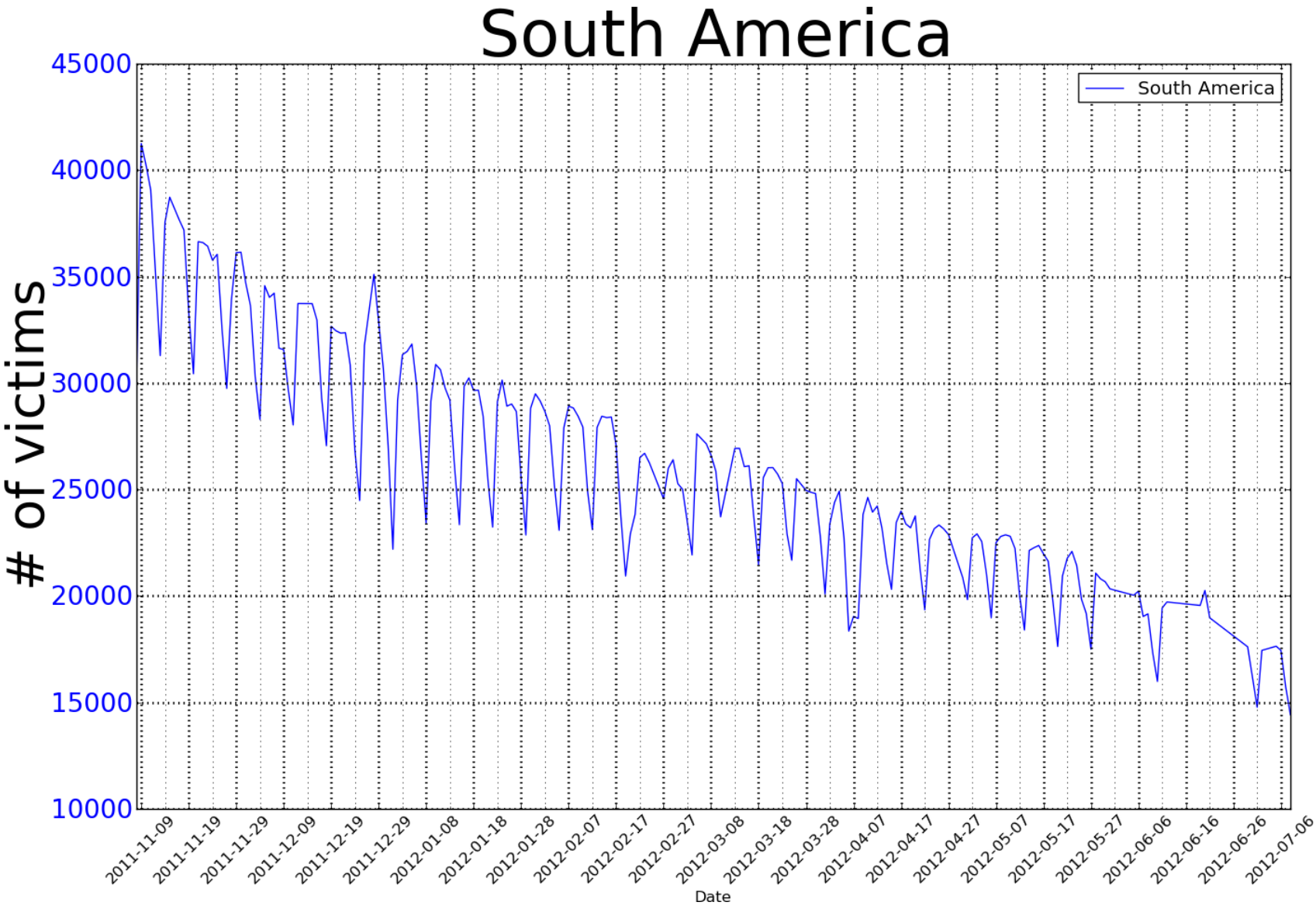
3. Statistics



3. Statistics



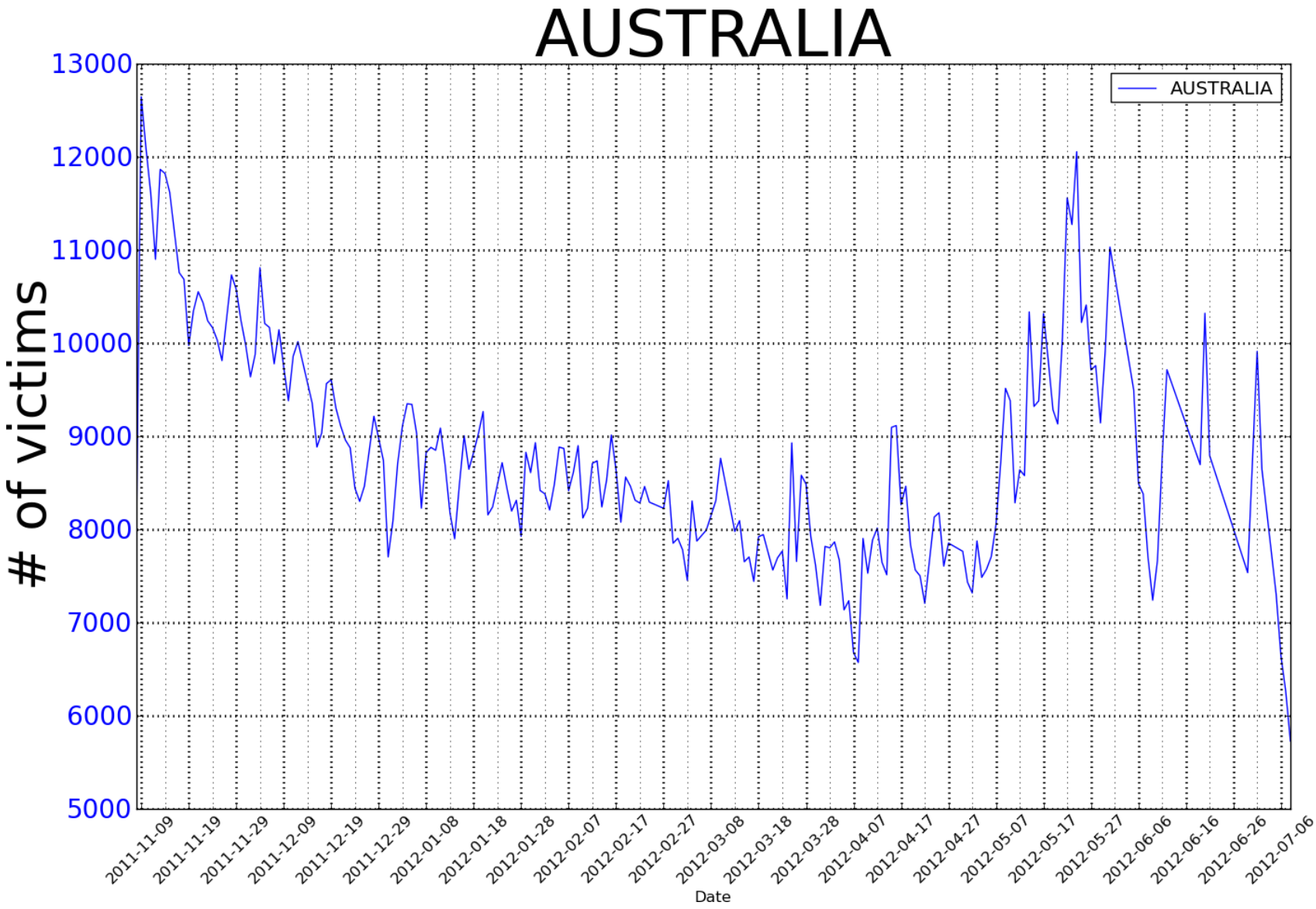
3. Statistics



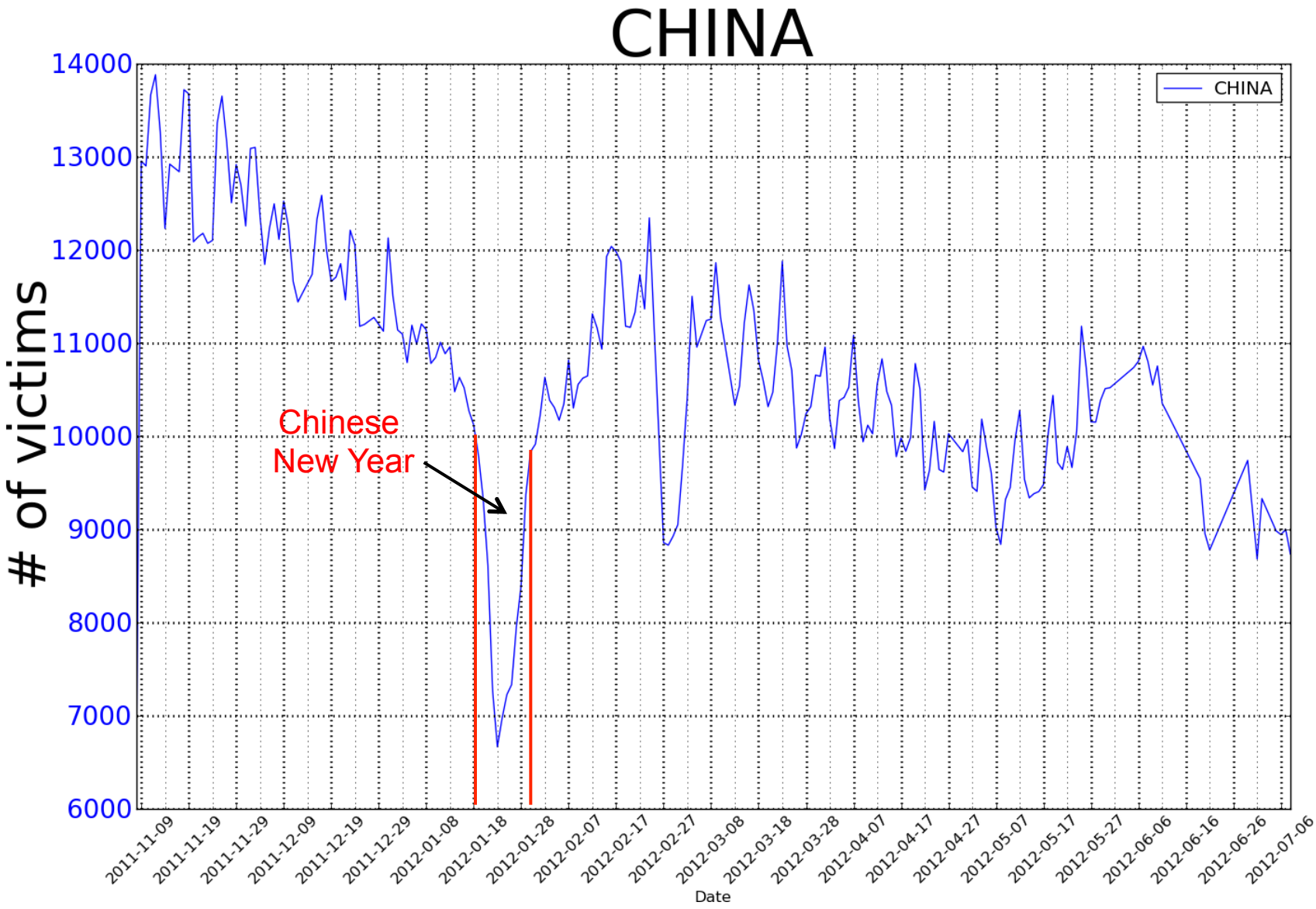
3. Statistics

- Top infected countries (based on daily count)

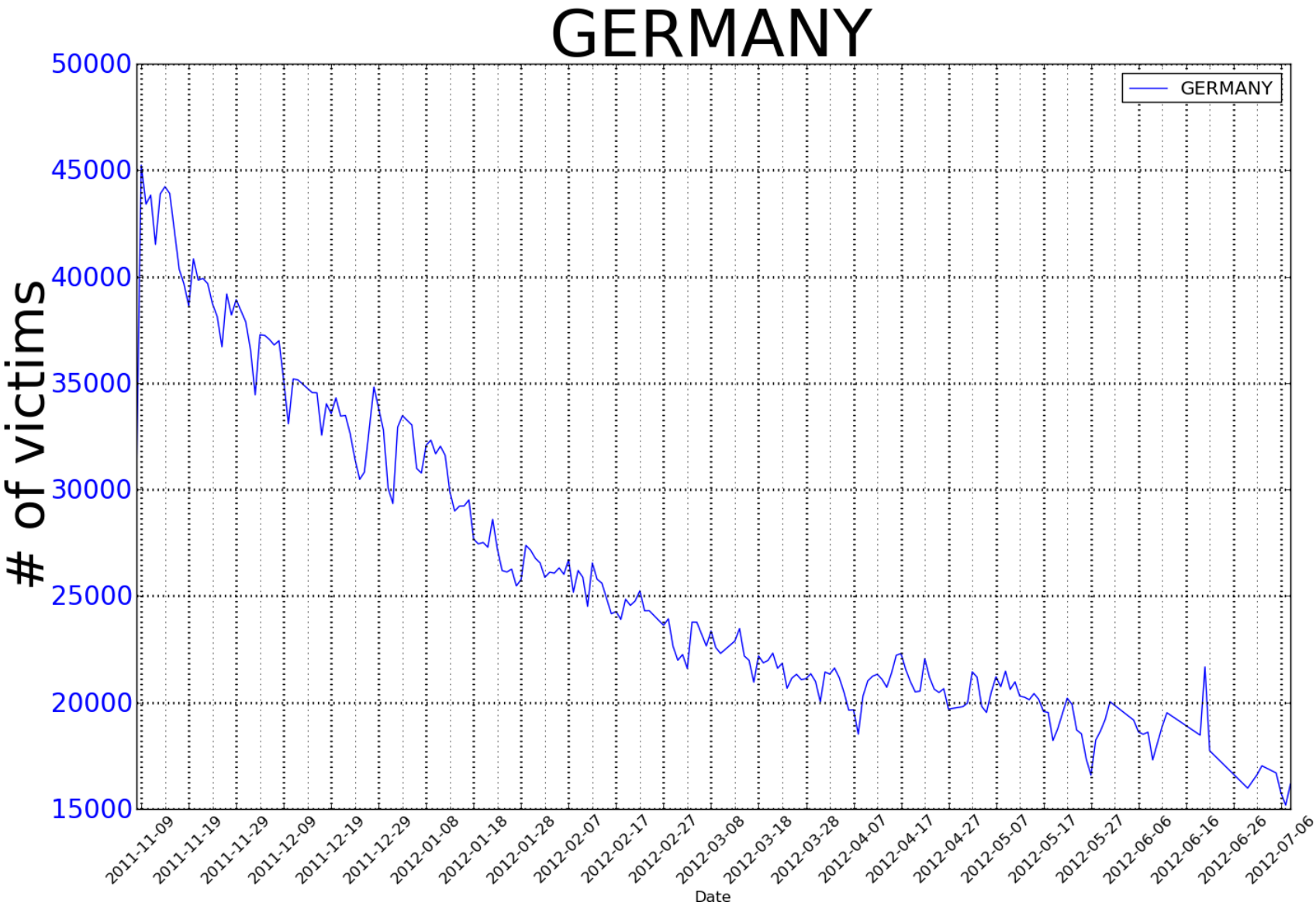
3. Statistics



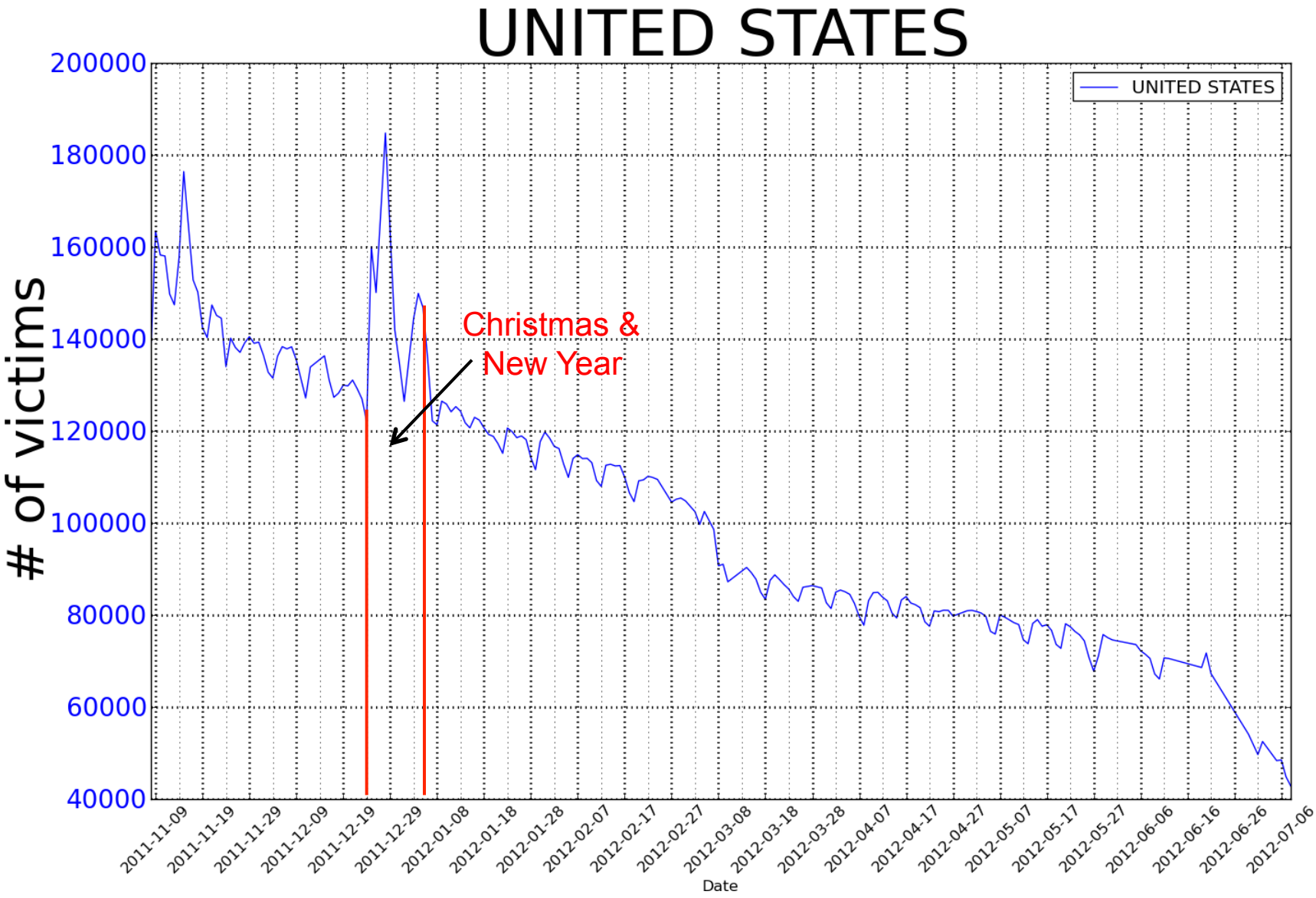
3. Statistics



3. Statistics



3. Statistics



3. Statistics

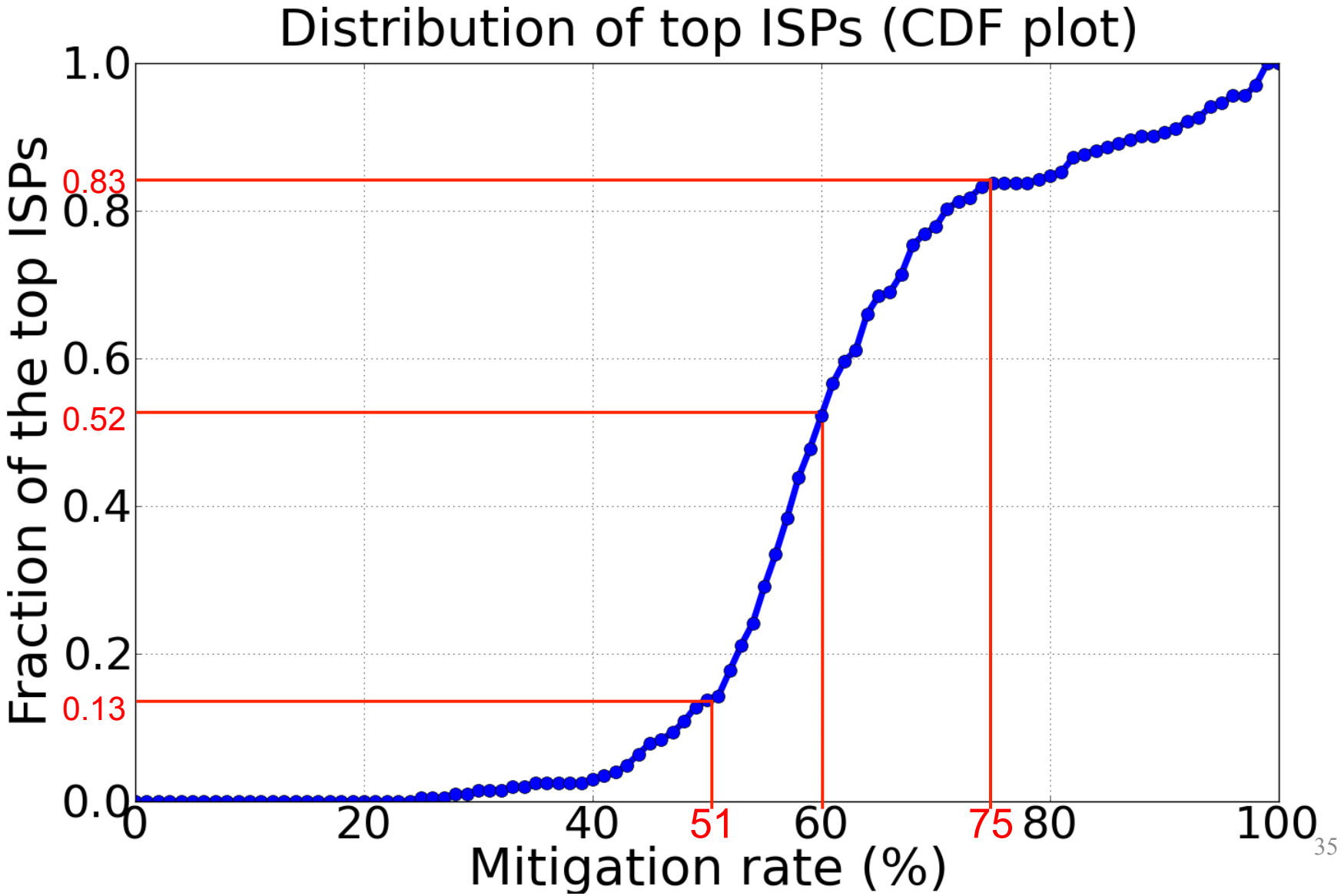
- Top infected ISPs
  - 203 distinct ISPs of which the maximum # of victims > 500
  - accounting for ~84% of all the infection around the world
  - most of them are North American and European ISPs

3. Statistics

- Mitigation rate
  - M: maximum victim count
  - A: the average of the last 7 days' victim counts
  - Mitigation rate = (M-A) / M * 100%

Mitigation Rate %	0-25	26-50	51-75	76-100
# of ISPs	0	26	143	34

3. Statistics



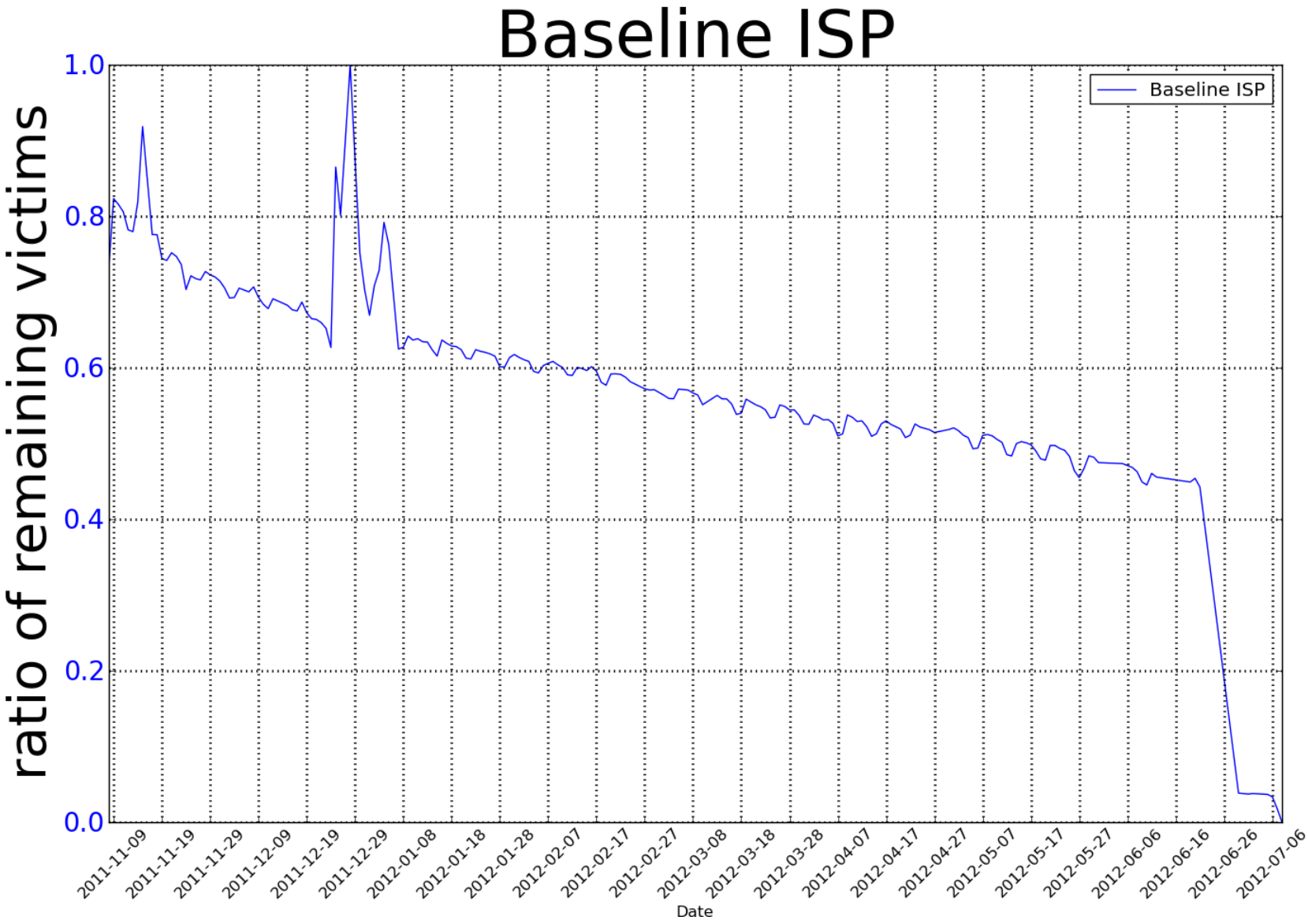
Outline

1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. Remediation Strategies for ISPs
6. Recommendation

4. Influence from Social Network & Online Media

- Baseline ISP
  - did nothing in terms of remediation before their redirection in June, 2012

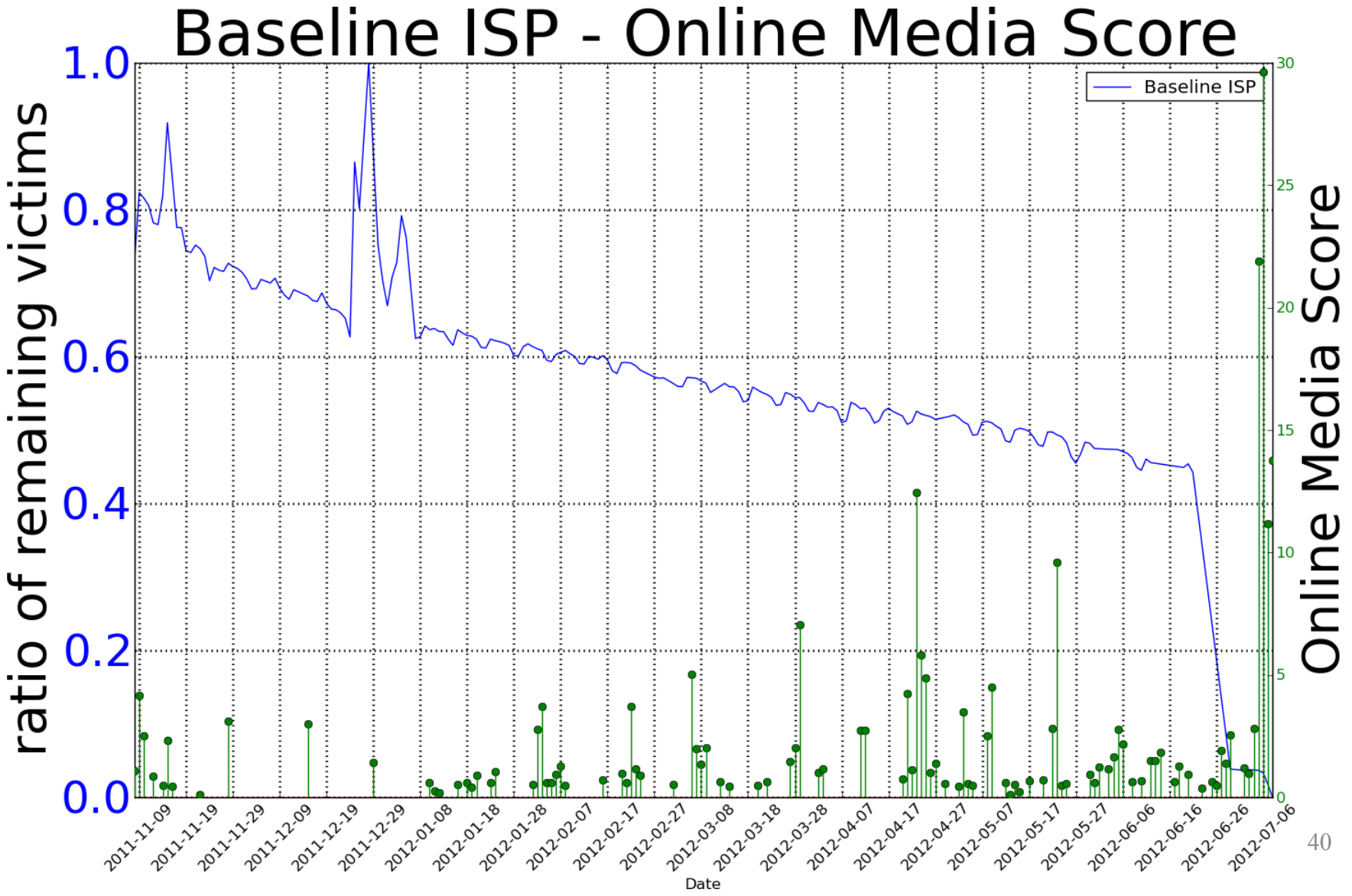
4. Influence from Social Network & Online Media



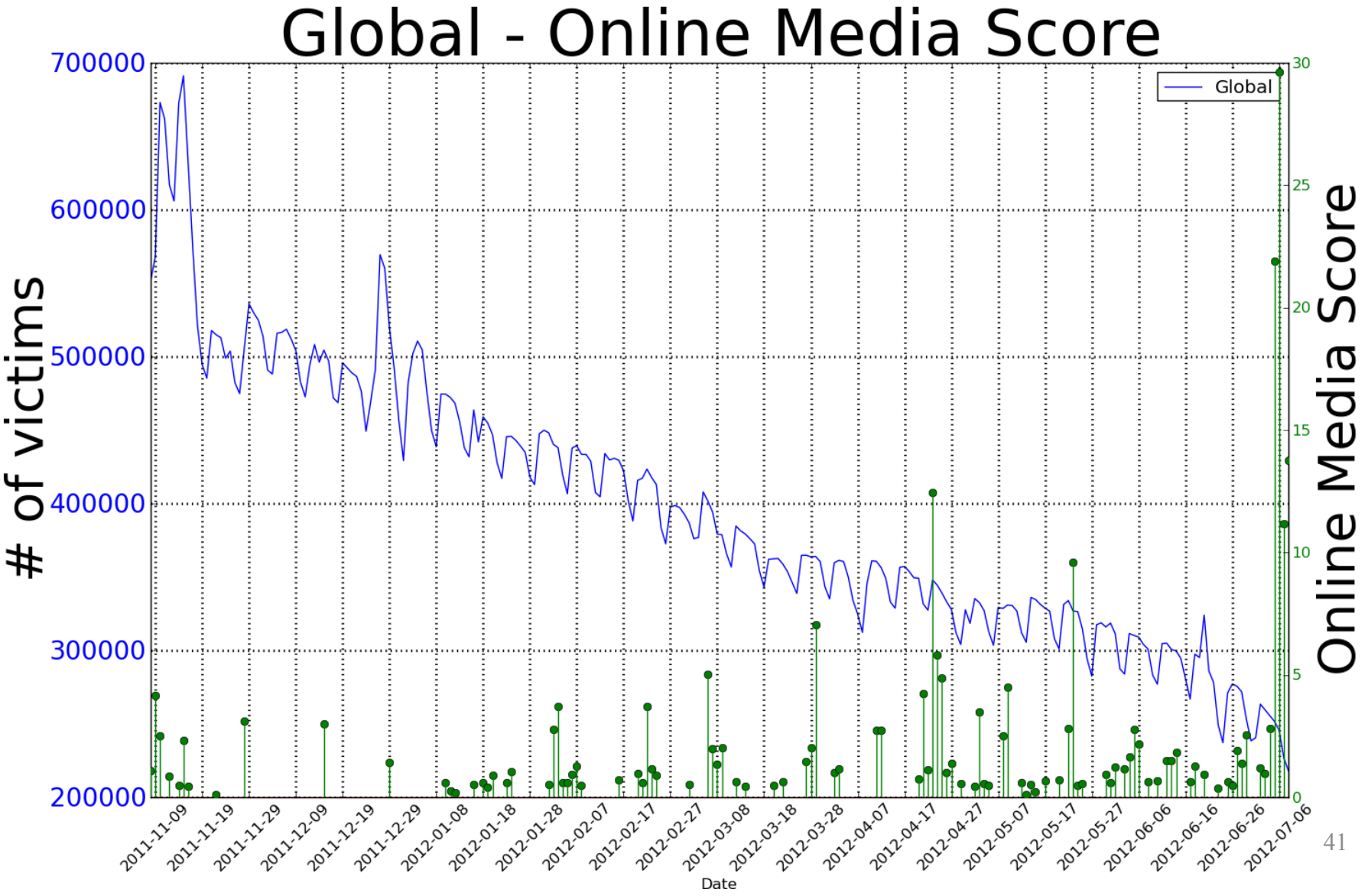
4. Influence from Social Network & Online Media

- Online Media
  - Metric – Online media score on Google search results of each day
  - Online Media Score:
    - summation of log(website reputation) for all websites

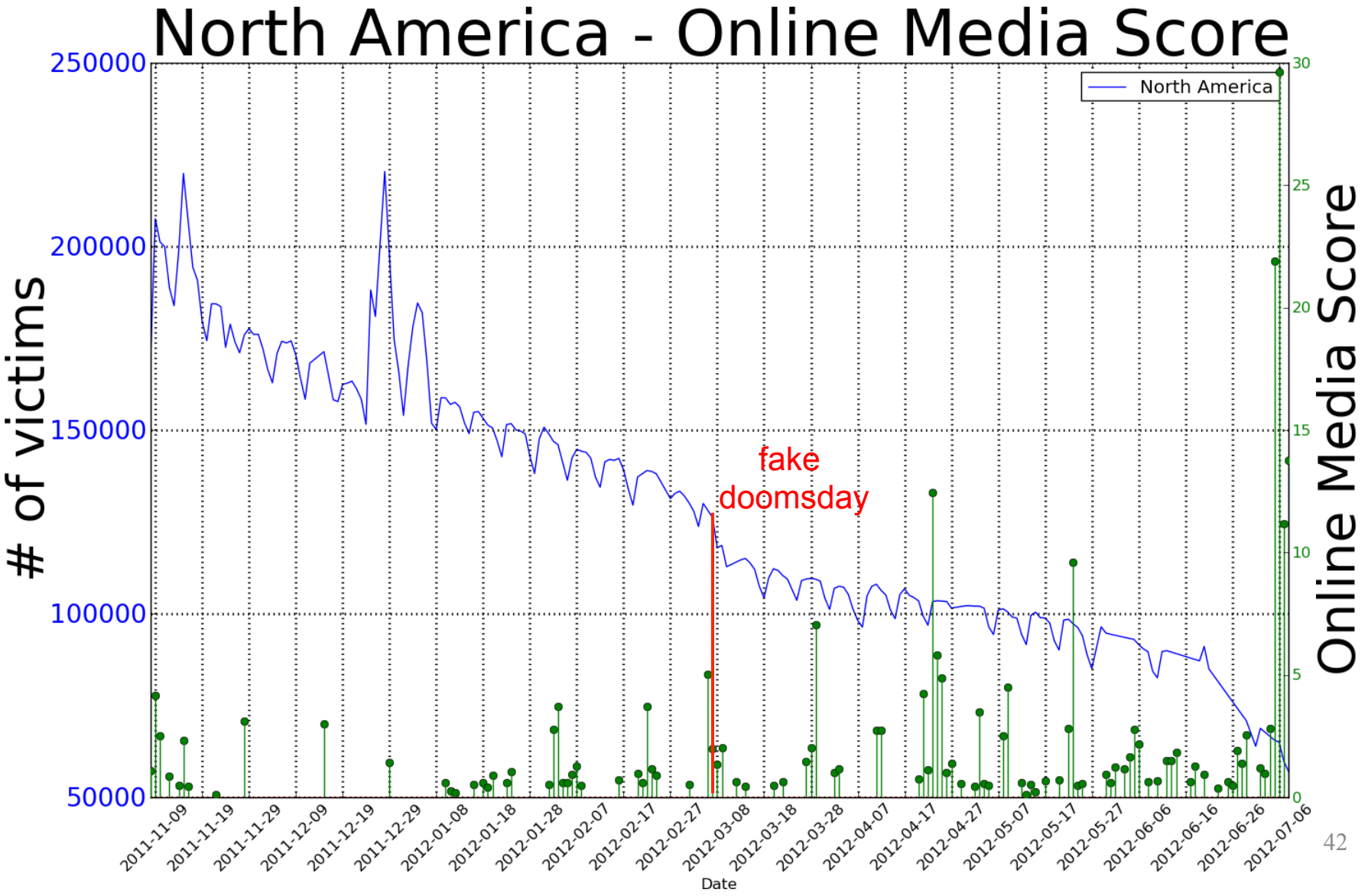
4. Influence from Social Network & Online Media



4. Influence from Social Network & Online Media



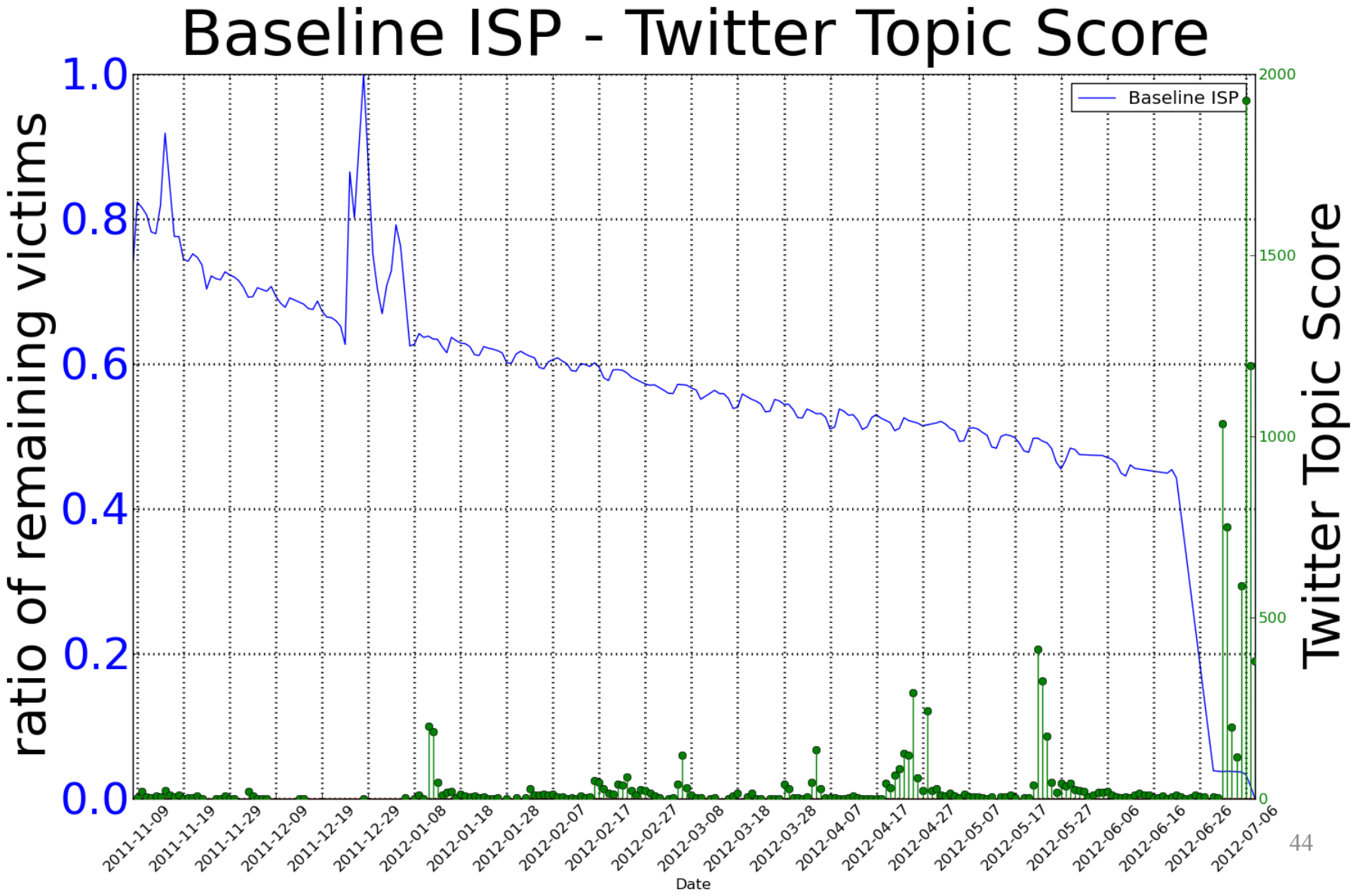
4. Influence from Social Network & Online Media



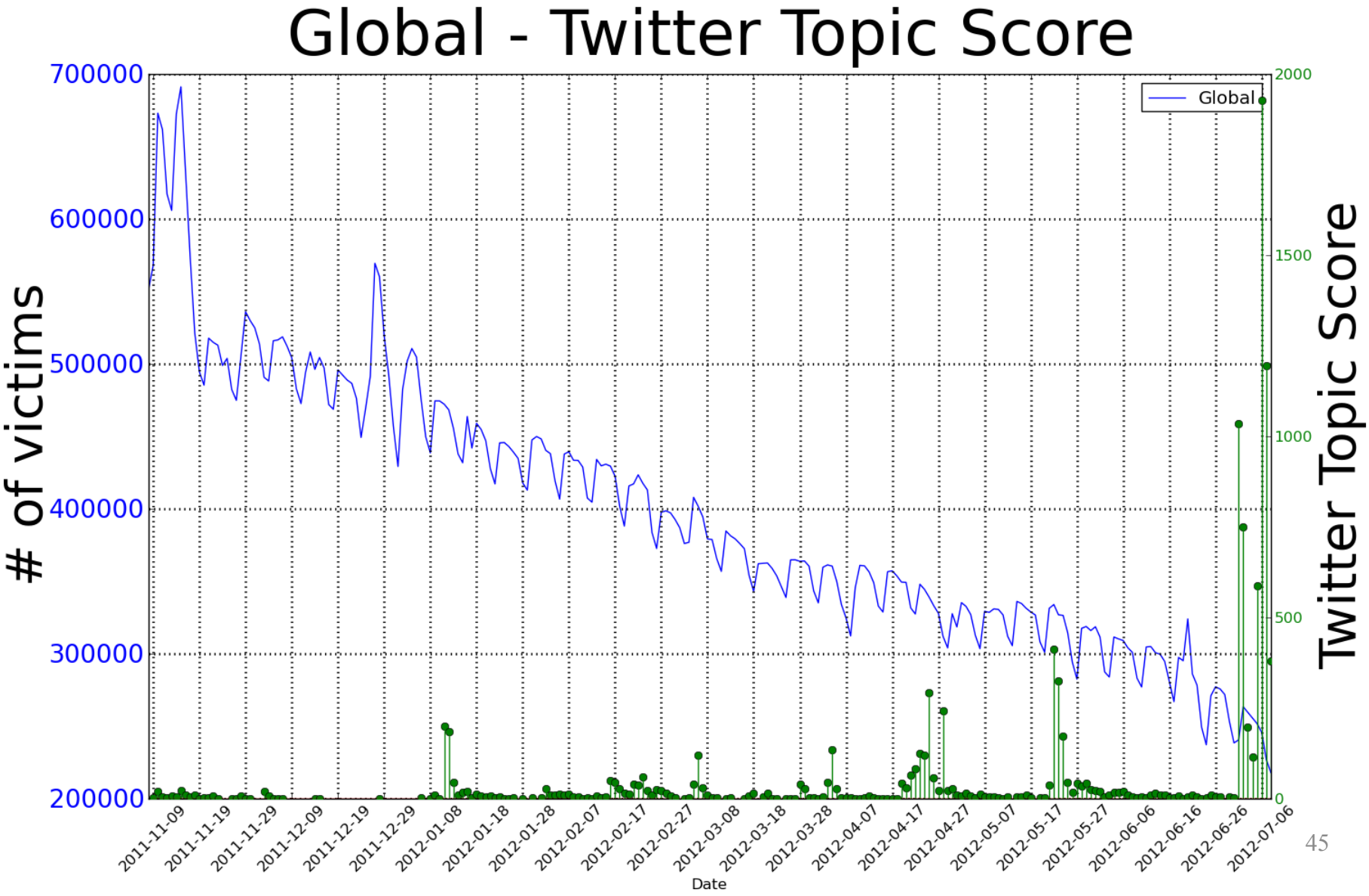
4. Influence from Social Network & Online Media

- Social Network – Twitter
  - Metric – Twitter Topic Score
    - summation of daily log(post count) multiplied by user's influential weight

4. Influence from Social Network & Online Media

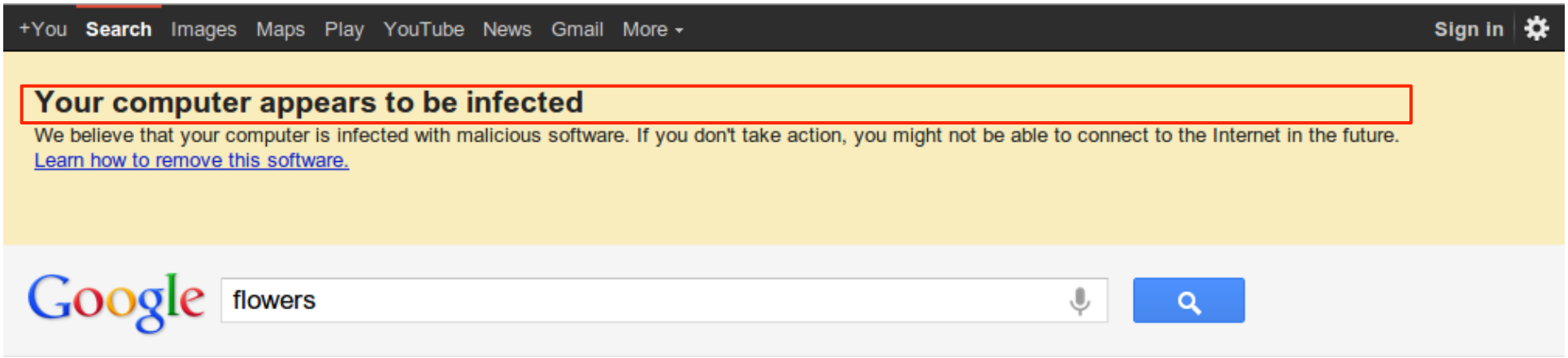


4. Influence from Social Network & Online Media



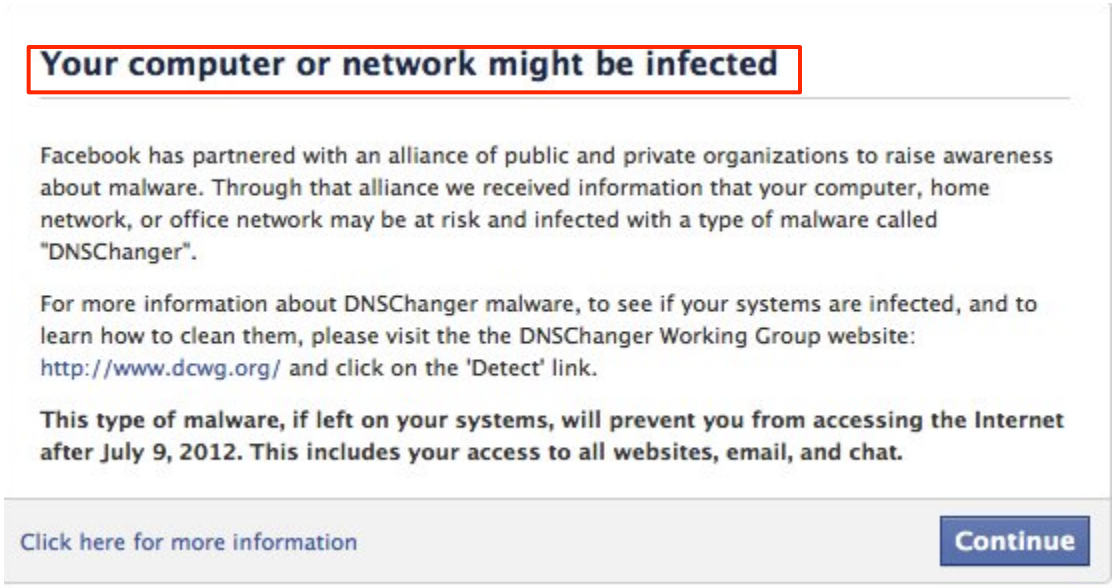
4. Influence from Social Network & Online Media

- Google's and Facebook's notifications
  - Google, May 22, 2012
    - Note: Active and direct to the victim notification



4. Influence from Social Network & Online Media

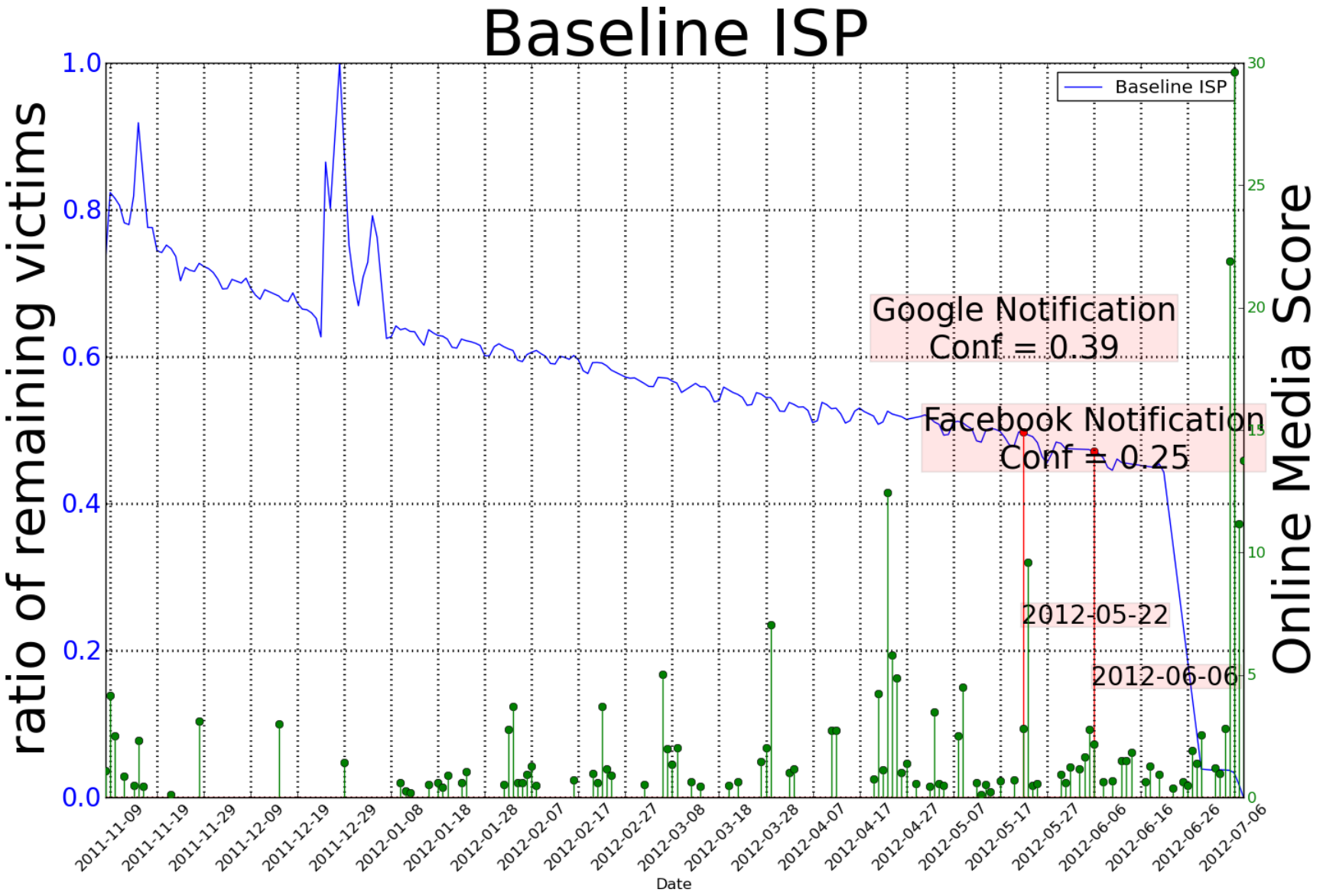
- Google's and Facebook's notifications
  - Facebook, June 6, 2012
    - Active notification



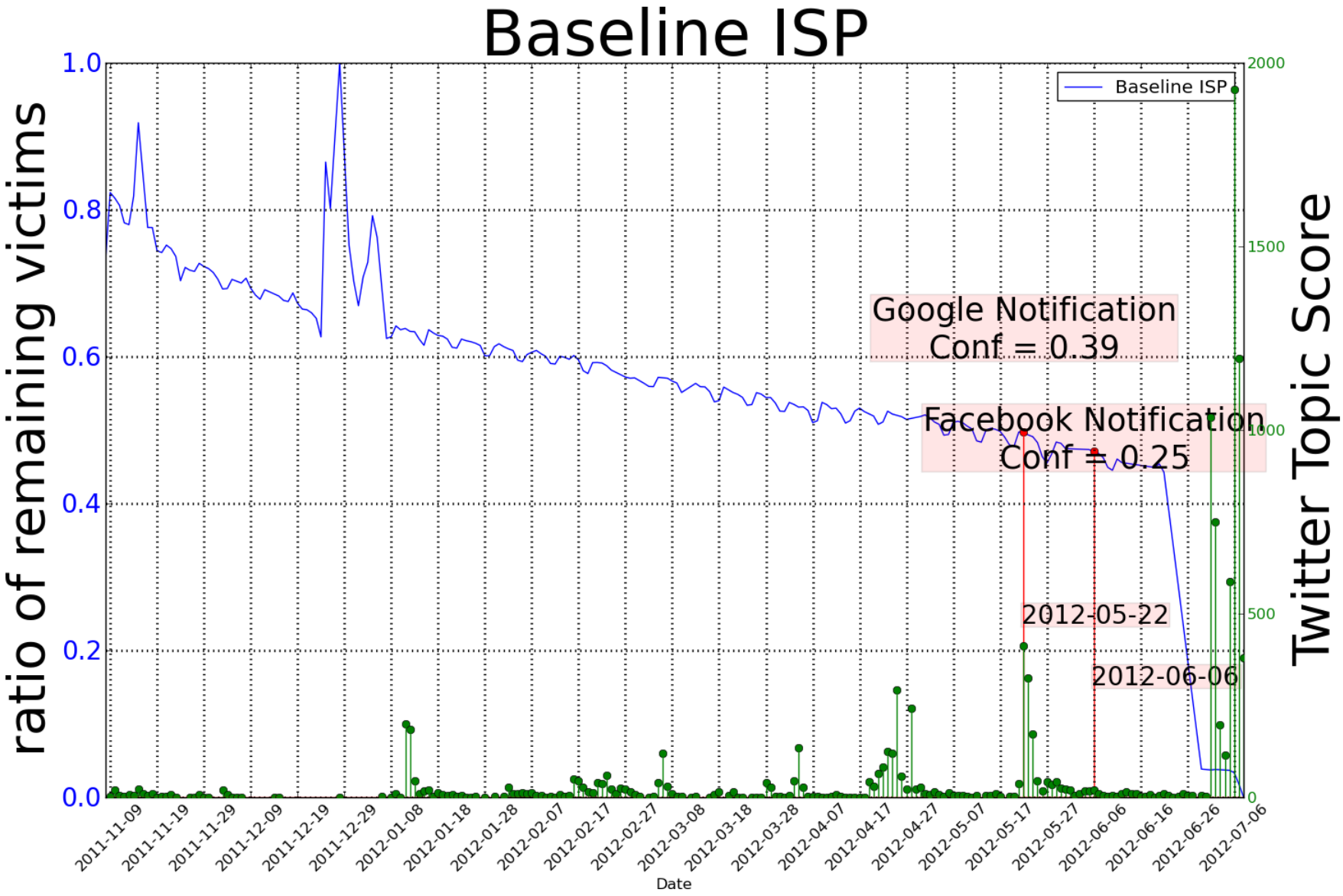
4. Influence from Social Network & Online Media

- Google's and Facebook's notifications
  - Metric – Confidence Score
    - Measures the *relative* victim population decrease rate within a time window
    - Indicates how effective the notification was
  - The higher the confidence score was, the more effective the notification was
    - > 0: above average
    - < 0: lower than average

4. Influence from Social Network & Online Media



4. Influence from Social Network & Online Media



4. Influence from Social Network & Online Media

- Summary
  - By correlating the victim population of North America and the world we see that online media – because of their specific messaging, e.g., “doomsday” – had impact on the victim population only several days before the DNS servers “turn off” dates
    - The “deadlines” set by FBI had an important role
  - Google’s direct notifications had positive impact even late in the process
    - We believe the impact would have been greater if done earlier

Outline

1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. Remediation Strategies for ISPs
6. Recommendation

5. Remediation Strategies for ISPs

- Survey from ISPs
  - Tried to reach 25 ISPs around the world
  - 9 responded

- Strategies summary
  - Notifications
    - Phone, E-mail, Help Pages…
  - Remediation approaches
    - DNS Redirection, Web Redirection, Walled Garden, MSRT, Anti-Virus software…

5. Remediation Strategies for ISPs

- Confidence Score of ISP Strategy
  - Measuring the effectiveness of strategies
    - One-time strategy confidence score:
      - describes how large the victim count decrease rate is within a time window (e.g. 10 days) since the strategy is taken
    - Period strategy confidence score:
      - describes how large the victim count decrease rate is within the period that the strategy is active

5. Remediation Strategies for ISPs

- Remediation Confidence Score
  - *Generally, the higher the remediation confidence score is, the more effective the strategy is*
  - One-time strategy
    - > 1: victim count decreases more quickly than the average rate
    - > 0: victim population decrease rate is above average
  - Period strategy
    - > 1: victim count has decreased more than expected

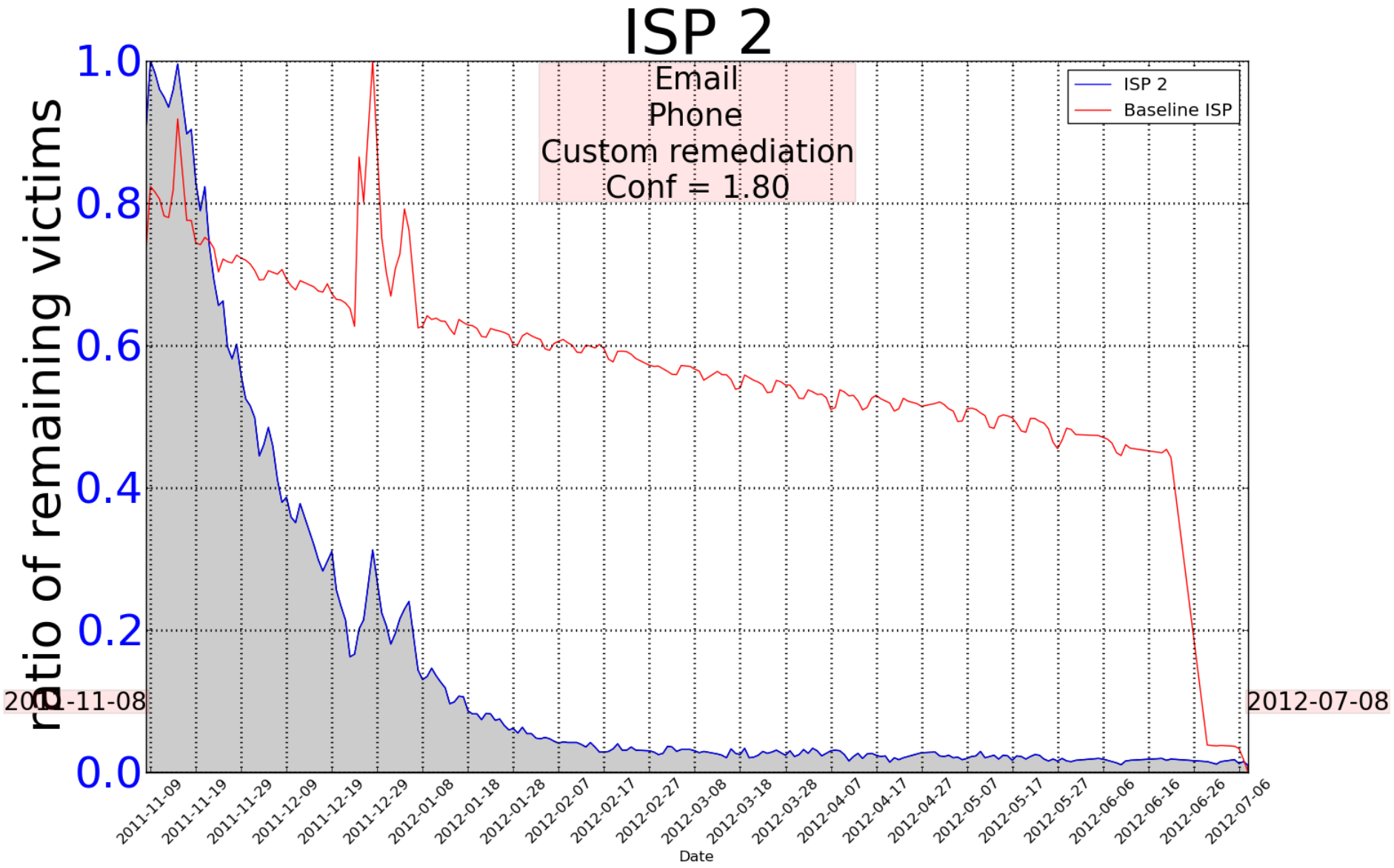
5. Remediation Strategies for ISPs

- Case study – ISP 2
  - Strategies taken over a period

Date	Strategy	Confidence Score
11/08/11 – 07/08/12	Email	1.80
11/08/11 – 07/08/12	Phone	1.80
11/08/11 – 07/08/12	Custom remediation	1.80

  - If there was no response to warnings, the customer's connectivity would be suspended so that they were forced to speak with a support staff
  - Advocated full format, partition recreation and OS reinstall in order to completely remediate the threat

5. Remediation Strategies for ISPs

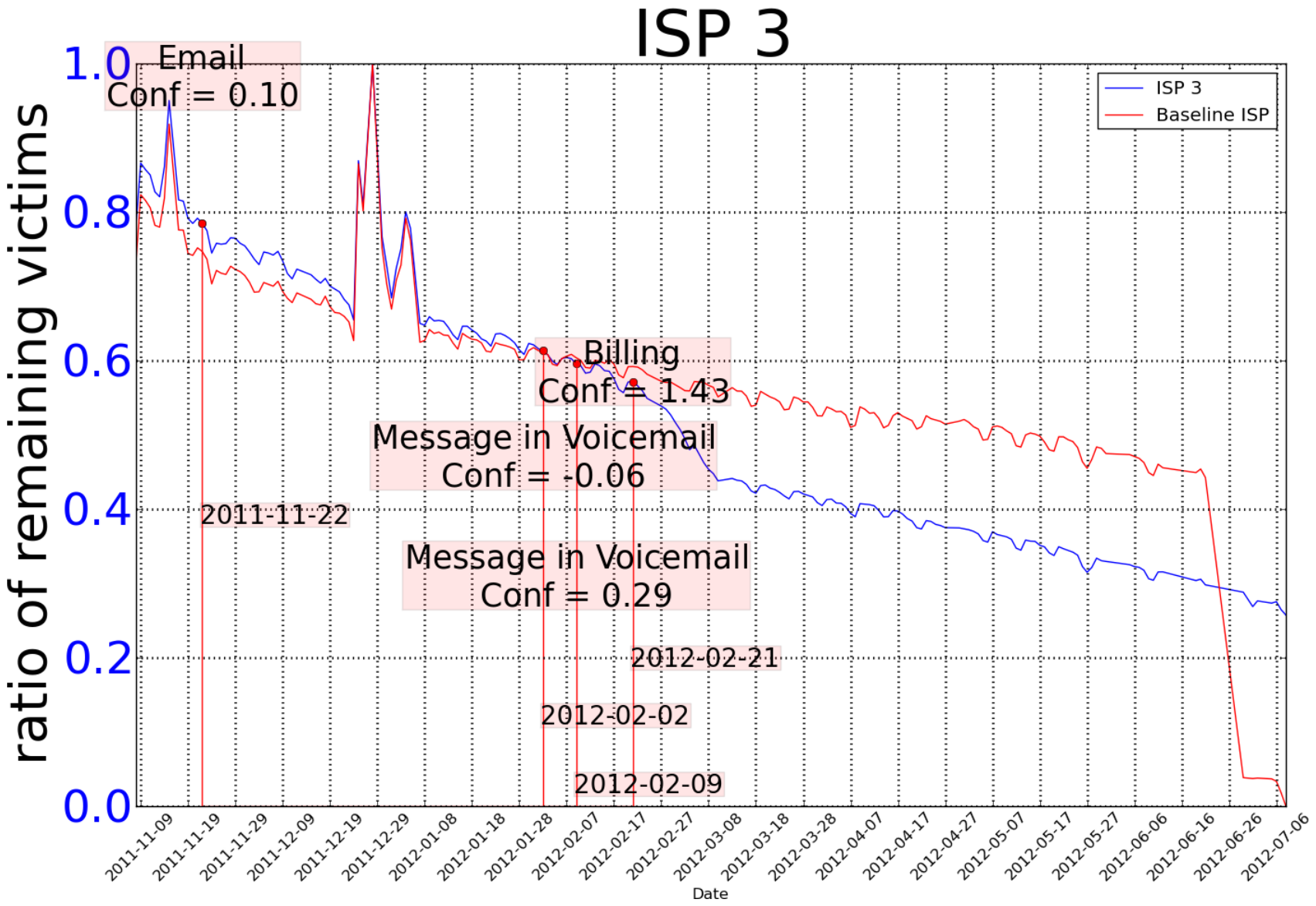


5. Remediation Strategies for ISPs

- Case study – ISP 3
  - Notifications on specific days (one-time strategy)

Date	Strategy	Confidence Score
2011-11-22	Email	0.10
2012-02-02	Message in Voicemail	-0.06
2012-02-09	Message in Voicemail	0.29
2012-02-21	Billing	1.43

5. Remediation Strategies for ISPs

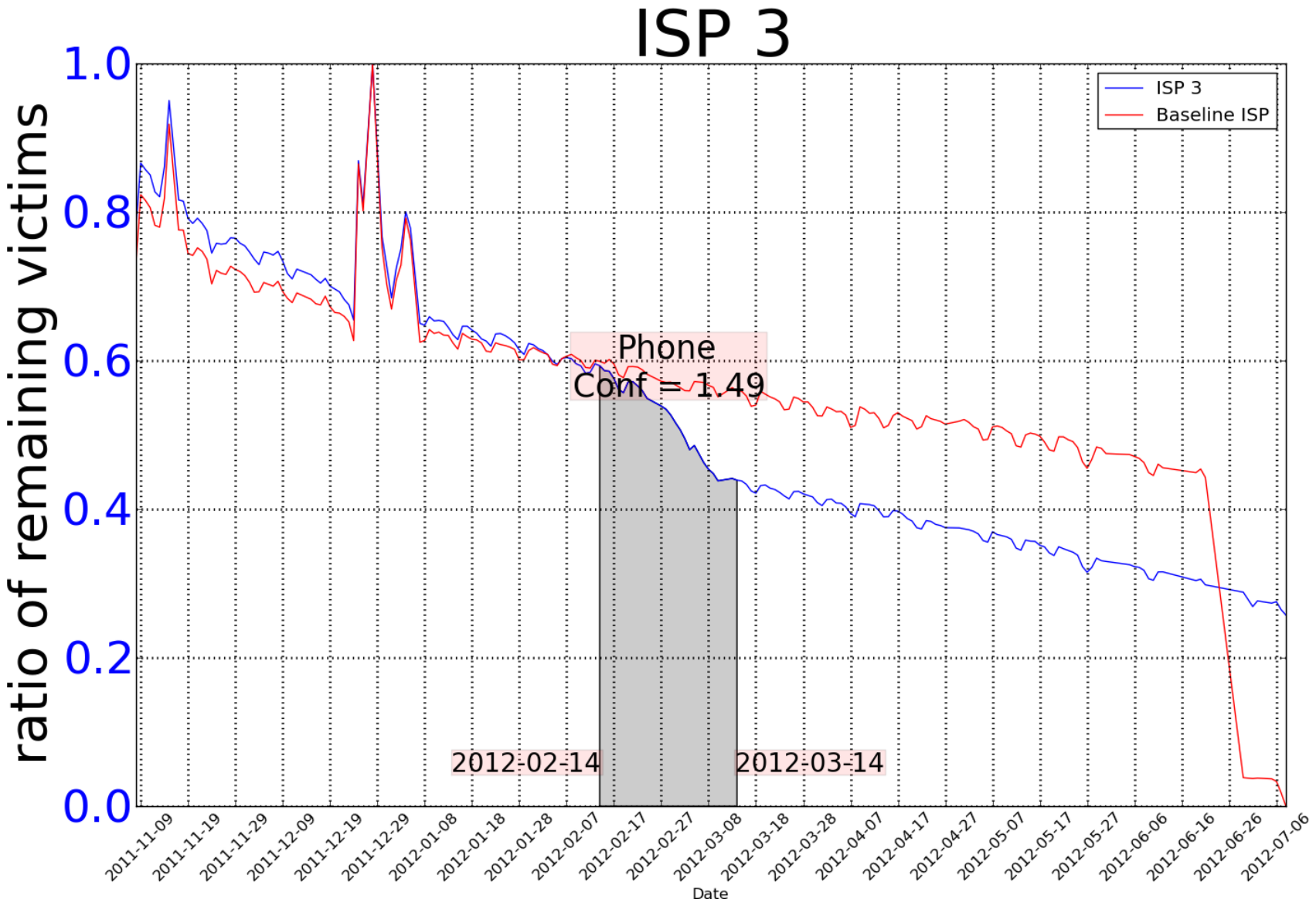


5. Remediation Strategies for ISPs

- Case study – ISP 3
  - Strategies taken over a period

Date	Strategy	Confidence Score
11/22/11 – 07/08/12	Anti-virus software	0.76
11/22/11 – 07/08/12	MSRT	0.76
12/03/11 – 01/12/12	Generic bot notification	0.72
01/13/12 – 02/20/12	Targeted bot notification	0.76
01/13/12 – 07/08/12	Custom remediation	0.73
02/14/12 – 03/14/12	Phone	1.49

5. Remediation Strategies for ISPs

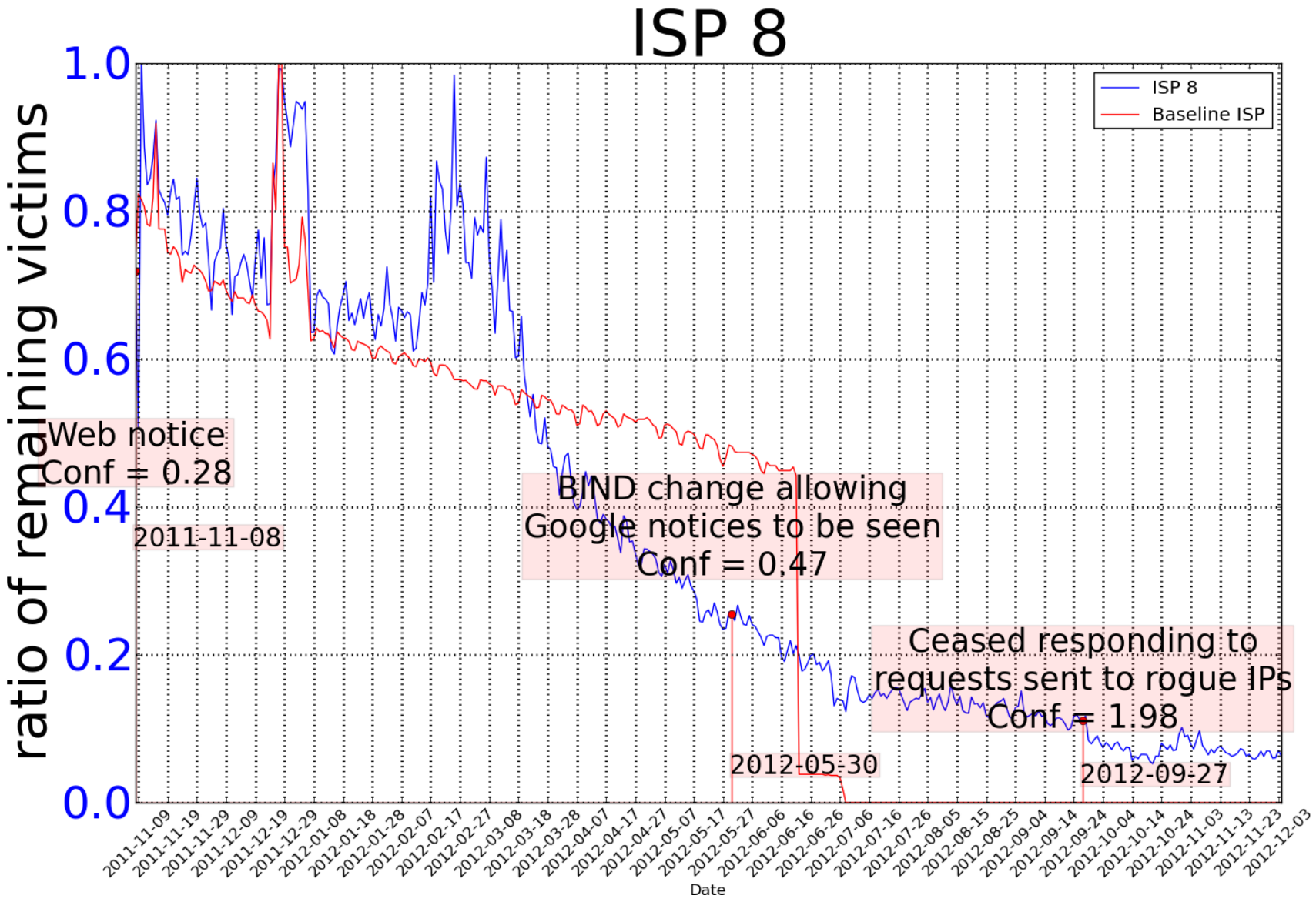


5. Remediation Strategies for ISPs

- Case study – ISP 8
  - Infection data directly received from ISP
  - One-time strategies

Date	Strategy	Confidence Score
2011-11-08	Web notice	0.28
2012-05-30	BIND change allowing Google notices to be seen	0.47
2012-09-27	Ceased responding to requests sent to rogue IPs	1.98

5. Remediation Strategies for ISPs

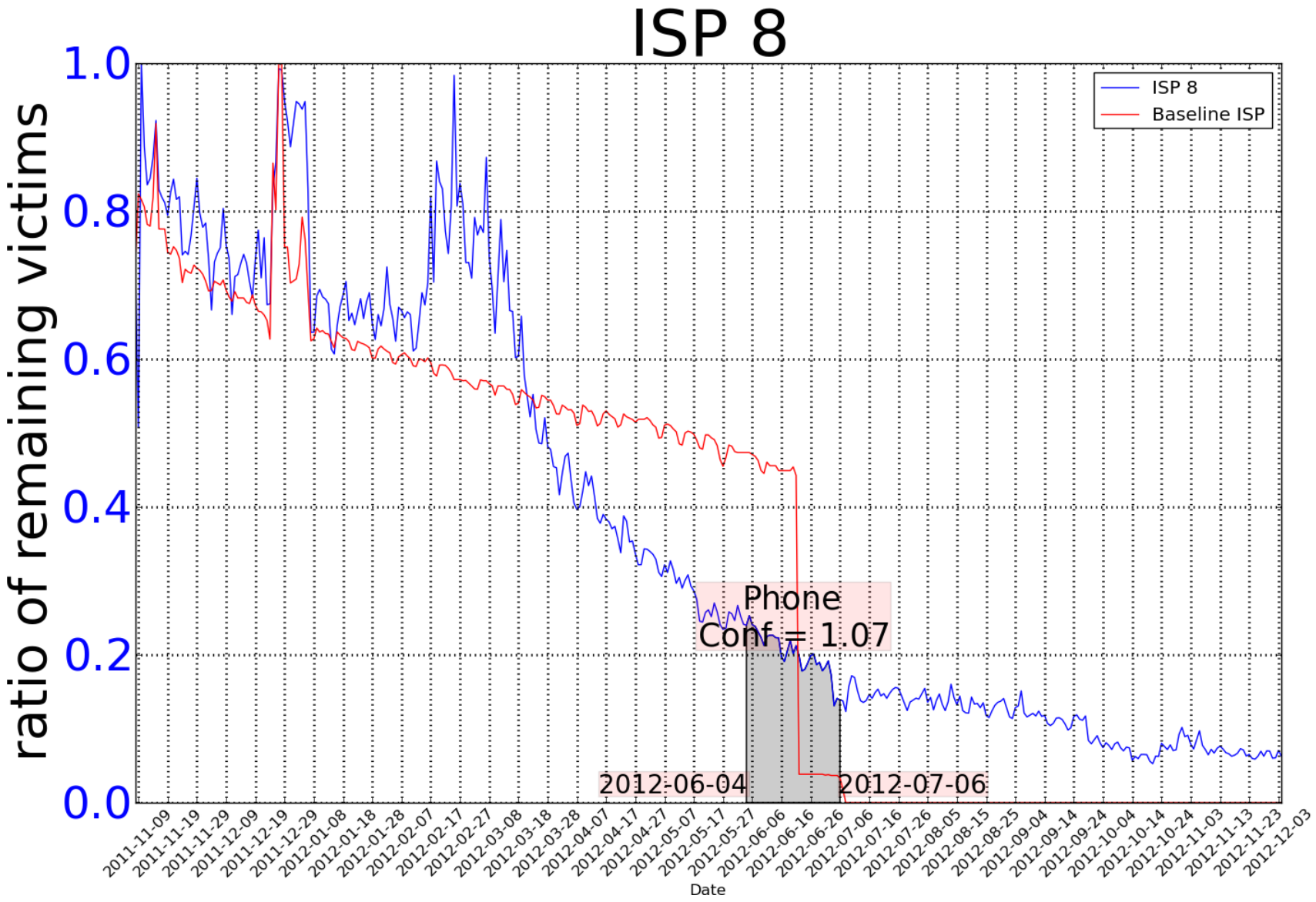


5. Remediation Strategies for ISPs

- Case study – ISP 8
  - Strategies taken over a period

Date	Strategy	Confidence Score
11/08/11 – 01/21/13	DNS redirection	0.78
12/09/11 – 12/12/11	Email	0.95
05/21/12 – 09/27/12	Mac Instruction	0.53
06/04/12 – 07/06/12	Phone	1.07
06/04/12 – 10/05/12	Anti-virus software	0.57
06/04/12 – 10/05/12	Custom remediation	0.57
08/21/12 – 09/27/12	Walled Garden/Web Redirection	0.54
08/21/12 – 09/27/12	Updating router/SOHO device DNS	0.54
08/21/12 – 09/27/12	Updating operating system DNS	0.54

5. Remediation Strategies for ISPs

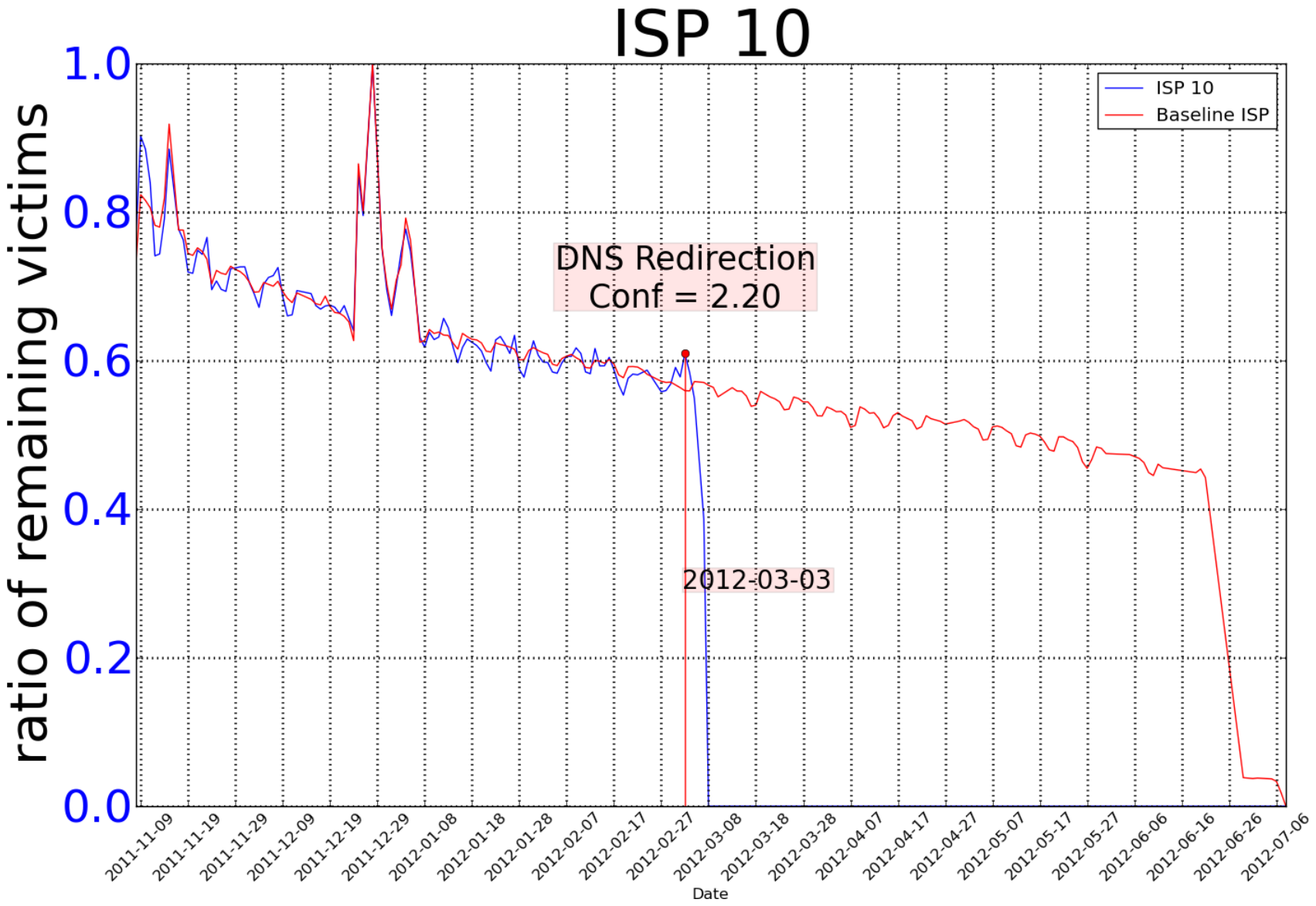


5. Remediation Strategies for ISPs

- Case study – ISP 10
  - DNS redirection on specific day
  - Infected customers were ultimately placed in a walled garden environment
  - Infected customers received a series of notifications via postal mail, voicemail, and email

Date	Strategy	Confidence Score
2012-03-03	DNS redirection	2.20

5. Remediation Strategies for ISPs



5. Remediation Strategies for ISPs

- Summary
  - Making phone calls is the most effective method of notification
  - In addition to phone calls, billing seems to be a promising method to notify customers
  - Emails and redirection to a customized web page are also good ways of notification
  - DNS redirection is most effective in terms of preventing users from communicating with rogue DNS servers
    - DNS redirection alone is not sufficient. Notifications are still needed since machines may still be infected with malware

Outline

1. Background & Motivation
2. Data & Methodology
3. Statistics
4. Influence from Social Network & Online Media
5. ISP Strategies
6. Recommendation

6. Recommendation

- ISPs should use a combination of strategies
- Online & social media should provide active, direct messages and warnings to users earlier in the process
- Need coordination of all parties (ISPs, media sites, LEOs) as early as possible in the process
- Need to collect better telemetry data during remediation for postmortem analysis

- The End
- Q & A

Reference

- Remediation Confidence Score
  - One-time Strategy
    - N: total number of days
    - W: window size
    - V[i]: victim count of day *i*
    - P[i]: the relative victim count decrease rate within *W* days since day *i*
      - P[i] = (V[i] – V[i+W]) / V[i] * 100%
    - M: average of (P[0], P[1], …, P[N-1])
    - Std: standard deviation of (P[0], P[1], …, P[N-1])

    - Confidence[i] = (P[i] – M) / Std

Reference

- Remediation Confidence Score
  - Period Strategy
    - N: total number of days
    - R: mitigation rate of the N days
    - start: *start date* of strategy
    - end: *end date* of strategy
    - V[i]: victim count of day i
    - O: the observed victim count decrease rate within period of [start, end]
      - O = (V[start] – V[end]) / V[start] * 100%
    - E: the expected victim count drop rate within the period
      - E = (end – start) / R * 100%
    - Confidence[i] = E / O * 100%