



Securing Your Web World



# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

*Raimund Genes, Anthony Arrott, and David Sancho  
Trend Micro*

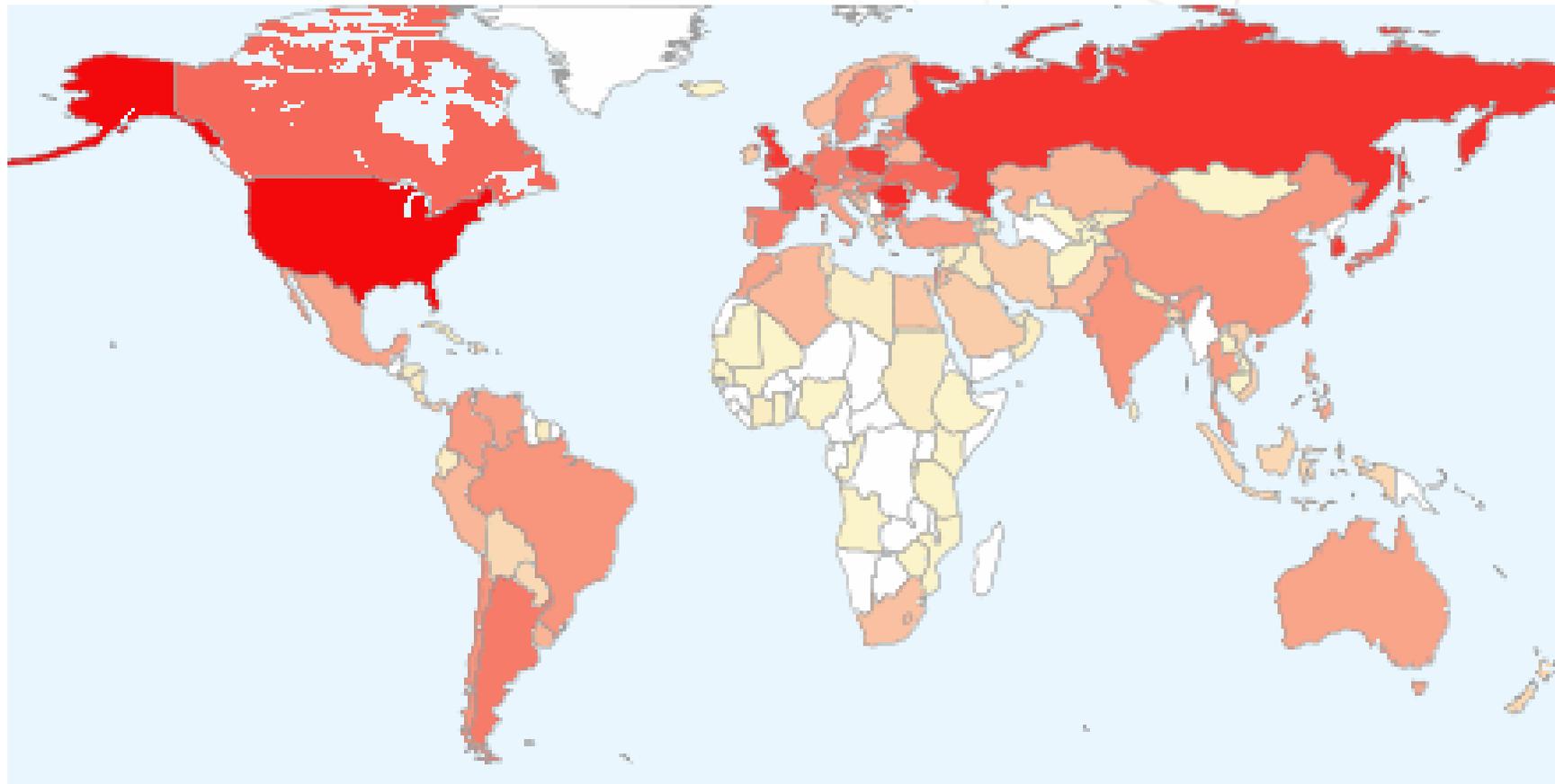
VB2008 - Ottawa

October 2008

# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

## Storm activity by country of IP source



## Stormy Weather

A quantitative assessment of the Storm web threat in 2007

Securing Your Web World

### How does Storm infect computers?

- Users open executable email attachments (e.g. 'Full Story.exe')

or

- Users visit infected websites (e.g. 'click\_for\_full\_story')
- Either way, user click results in becoming a remotely-controlled botnet zombie

# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

Securing Your Web World

## What does Storm do to make money for its perpetrators?

- 'Botnets for rent' in underground economy
- Rented botnets used:
  - as spam engines
  - in denial of service attacks
- Sell mined zombie data (e.g. address book contents)

## Stormy Weather

A quantitative assessment of the Storm web threat in 2007

Securing Your Web World

### How does Storm protect itself from detection & removal?

- Infects host zombies with rootkits
- Provides periodic updates of malware code
- Botnets configured
  - decentralized control
  - rotating activation
  - enhanced encryption
  - frequent code replacement

# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

Securing Your Web World

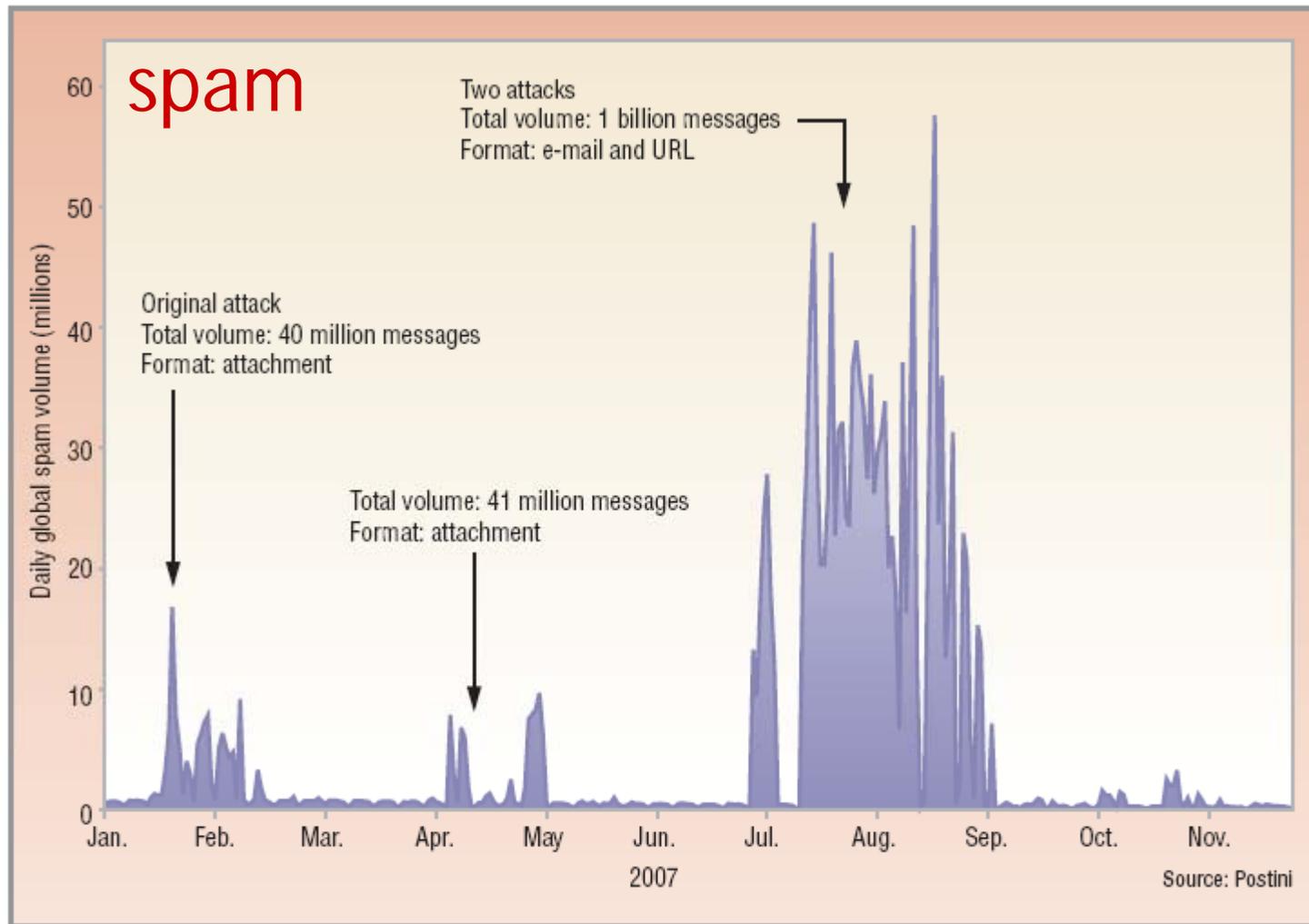
## Storm outbreaks in 2007

- 17 Jan 07 - "European Storm" Spam
- 12 Apr 07 - "Worm Alert" Spam
- 27 Jun 07 - "E-card" (applet.exe)
- 4 July 07 - "231st B-day"
- 2 Sep 07 - "Labor Day" (labor.exe)
- 5 Sep 07 - "Tor Proxy"
- 10 Sep 07 - "NFL Tracker"
- 17 Sep 07 - "Arcade Games"

Adopted from: Porras, Saidi & Yagneswaran

# Stormy Weather

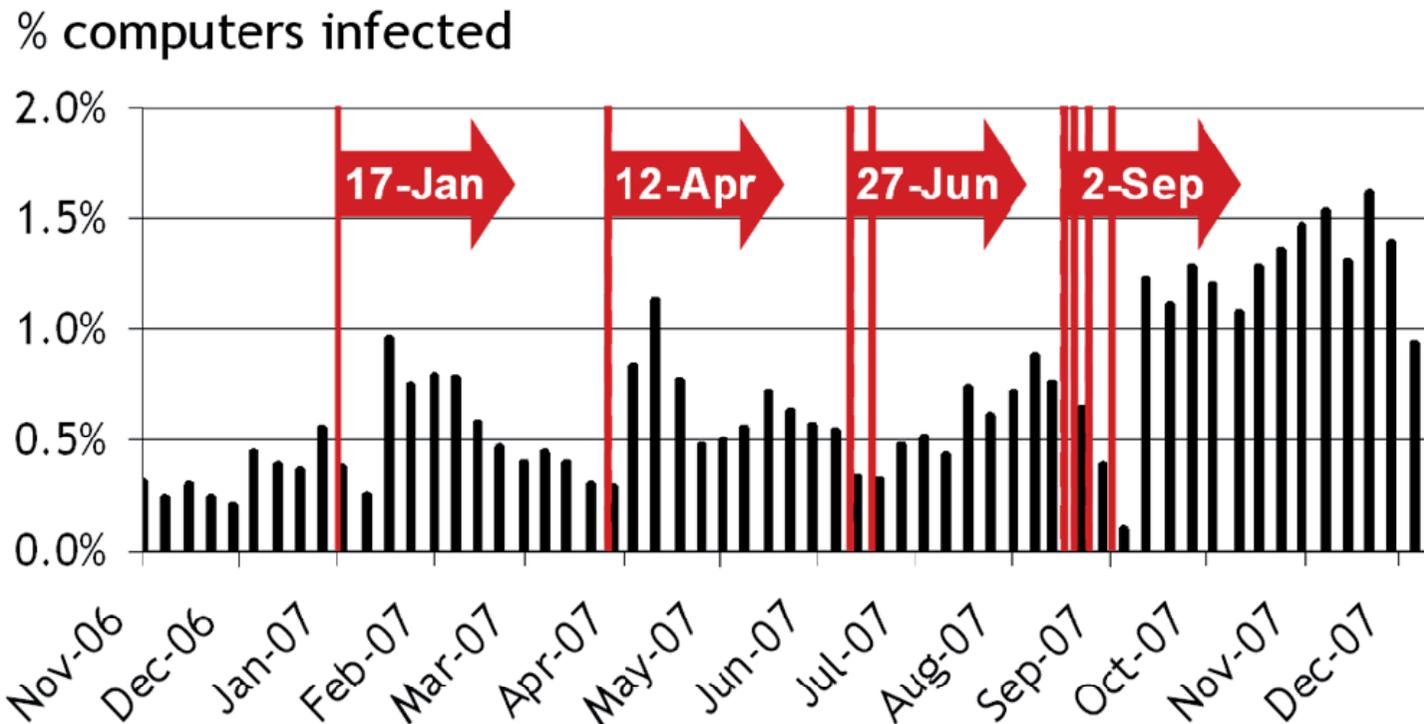
A quantitative assessment of the Storm web threat in 2007



# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

## Detections of Storm-related malware files



source: Trend Micro

# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

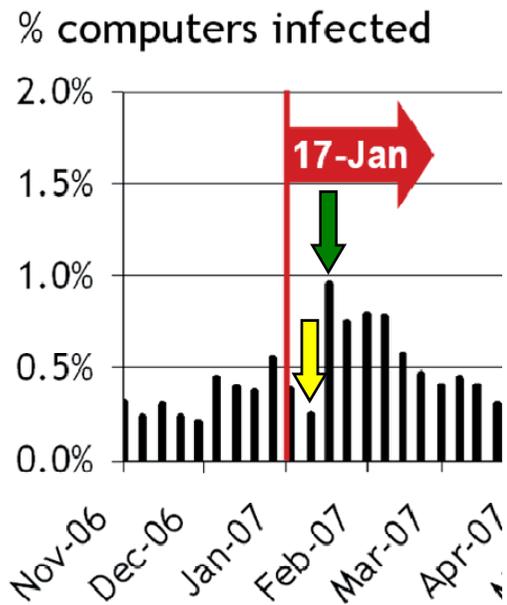
## Delay after 17-Jan-07

malware detection

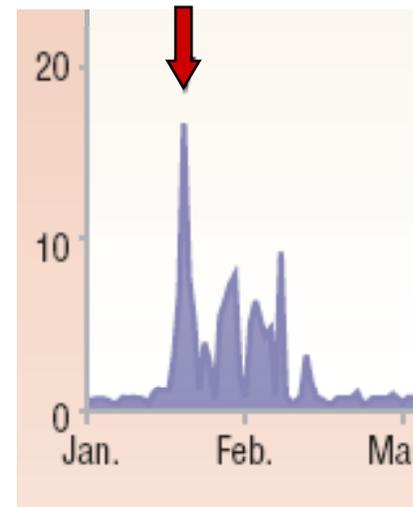
trough  2 weeks

peak  3 weeks

peak spam  1 week



## spam volume



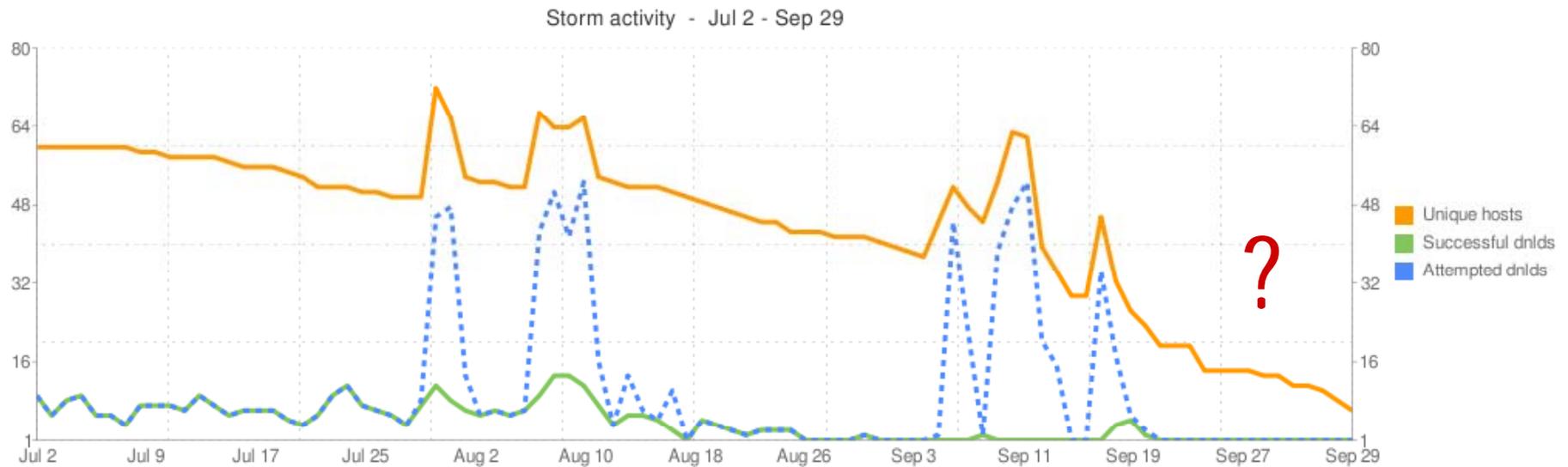
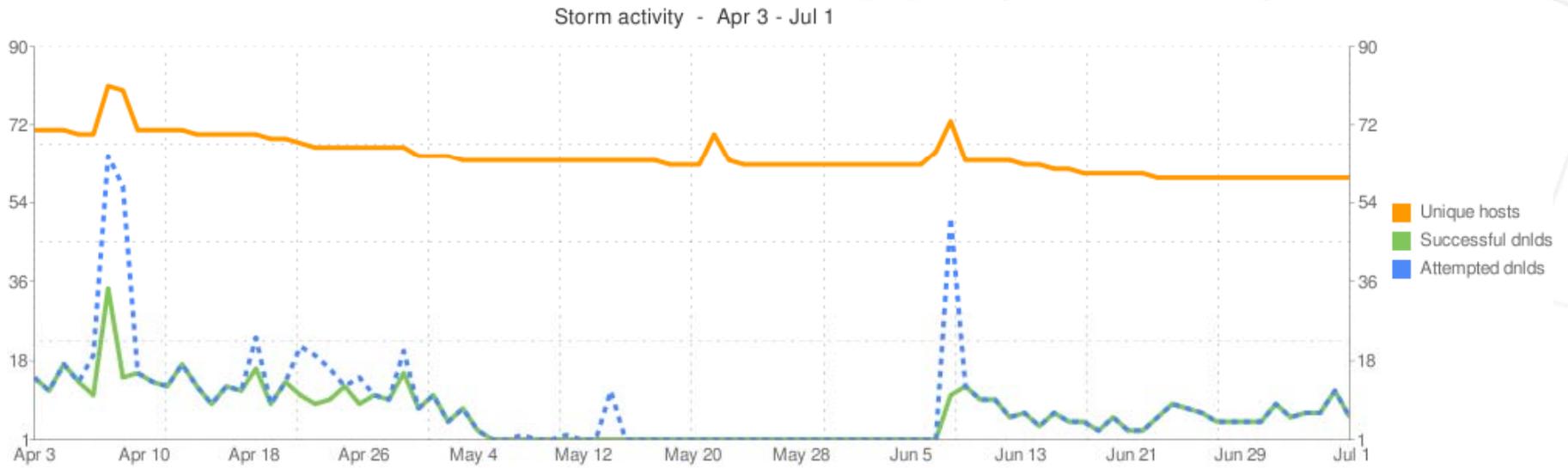
# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

<b>Delay after 17-Jan-07</b> malware detection trough  2 weeks peak  3 weeks peak spam  1 week	January 2007 Storm Attacks ("European Storm")
<b>Delay after 12-Apr-07</b> malware detection trough  1 week peak  3 weeks peak spam  3 weeks	April 2007 Storm Attacks ("Worm Alert")
<b>Delay after 27-Jun-07</b> malware detection trough  1 week peak  8 weeks peak spam  7 weeks	June/July 2007 Storm Attacks ("E-card", "231 <sup>st</sup> B-day")
<b>Delay after 2-Sep-07</b> malware detection trough  2 weeks peak  12 weeks peak spam [not available]	September 2007 Storm Attacks ("Labor Day", "Tor Proxy", "NFL Tracker", "Arcade Games")

# Stormy Weather

A quantitative assessment of the Storm web threat in 2007





Securing Your Web World



Thank you

VB2008 - Ottawa

October 2008