Stormy Weather

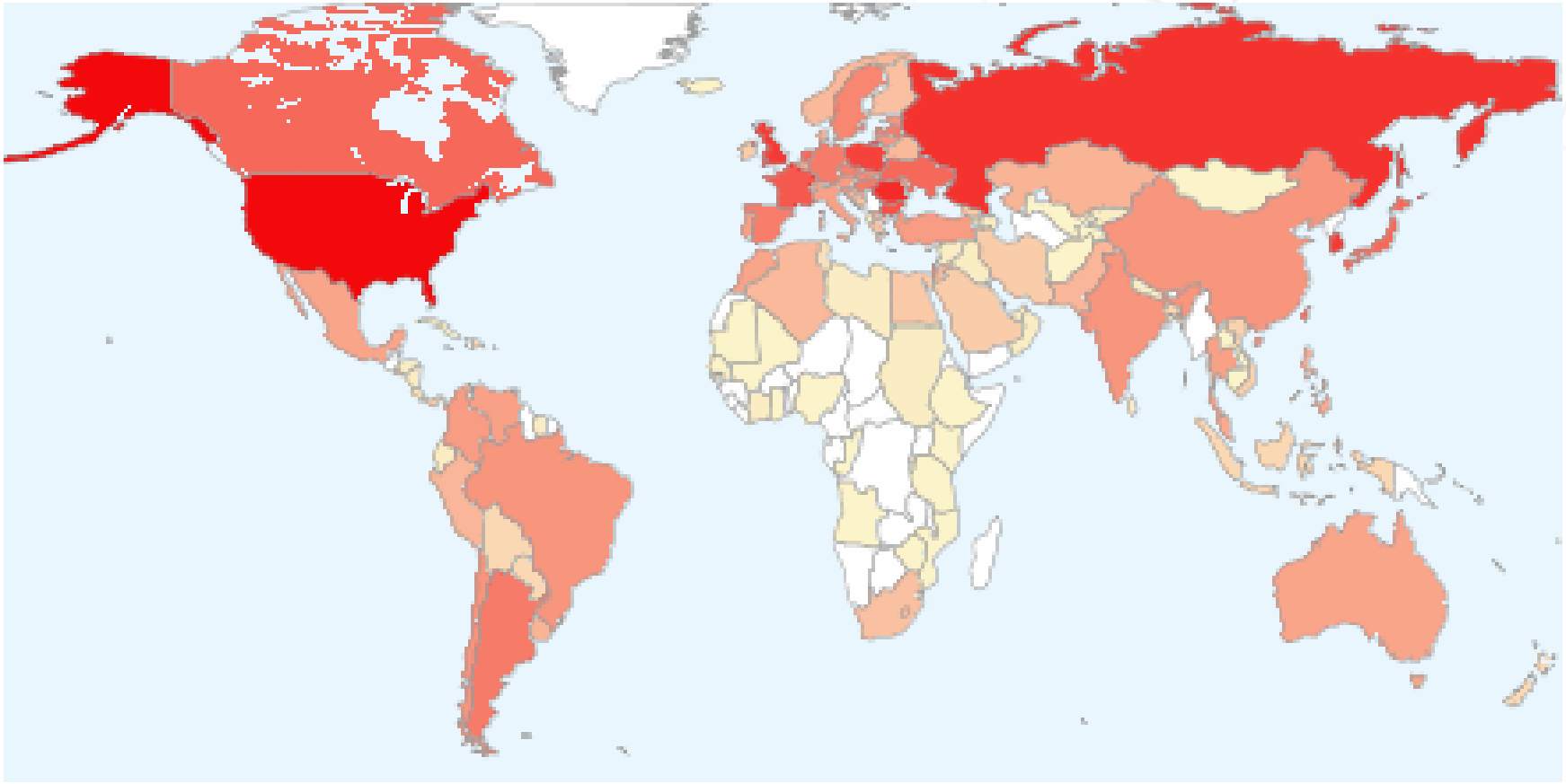
A quantitative assessment of the Storm web threat in 2007

Raimund Genes, Anthony Arrott, and David Sancho
Trend Micro

VB2008 - Ottawa

October 2008

Storm activity by country of IP source



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

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)

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

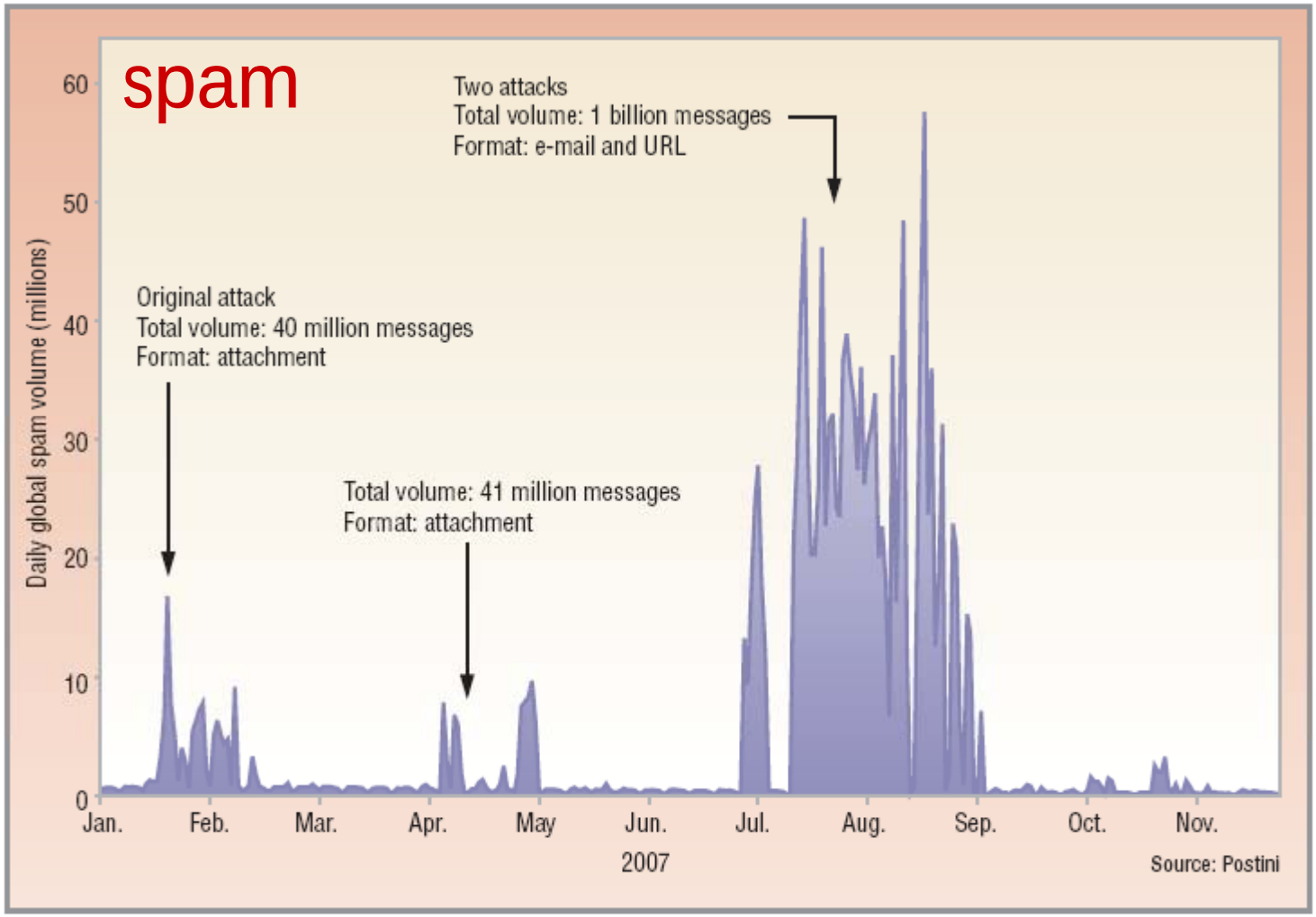
Storm outbreaks in 2007

- 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

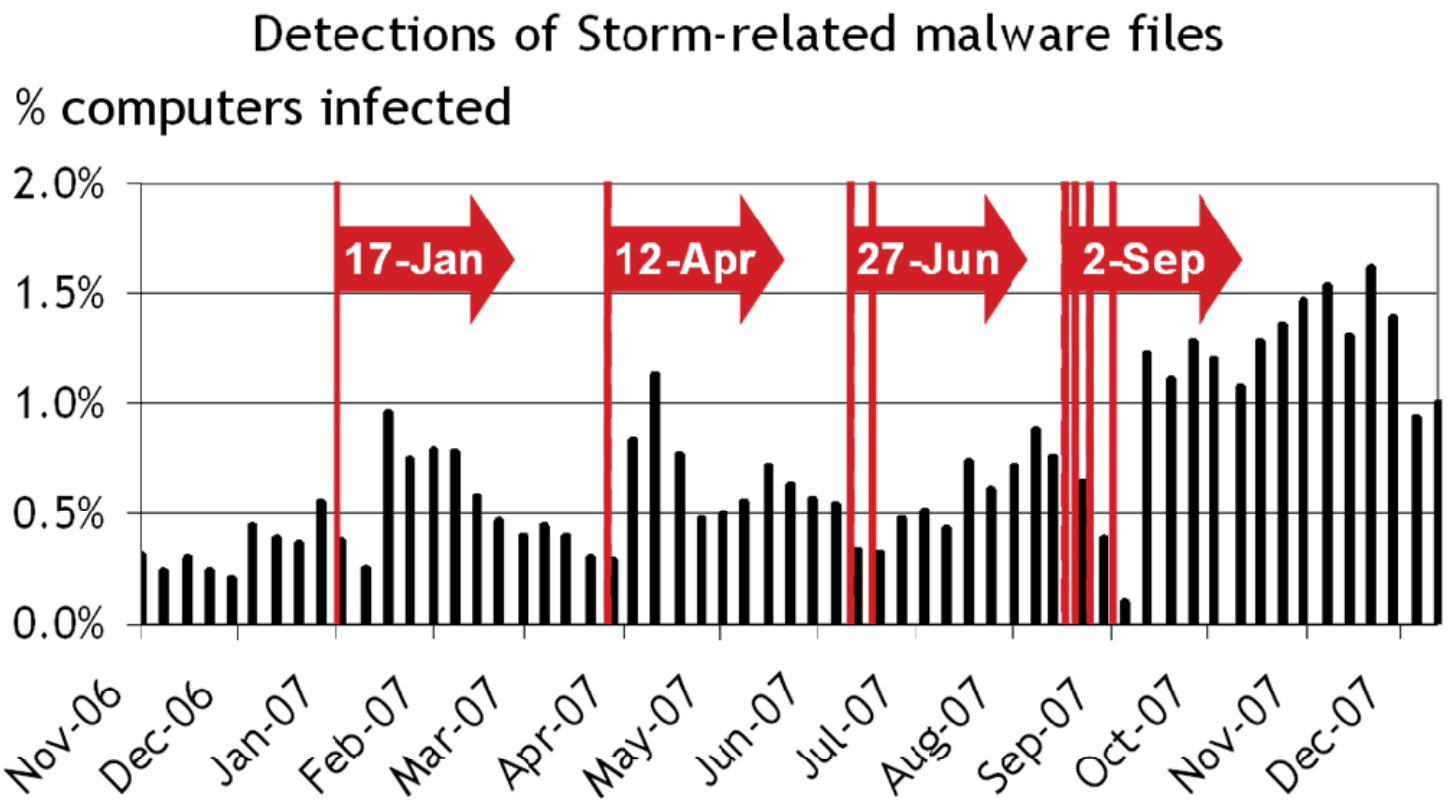
Stormy Weather

A quantitative assessment of the Storm web threat in 2007



Stormy Weather

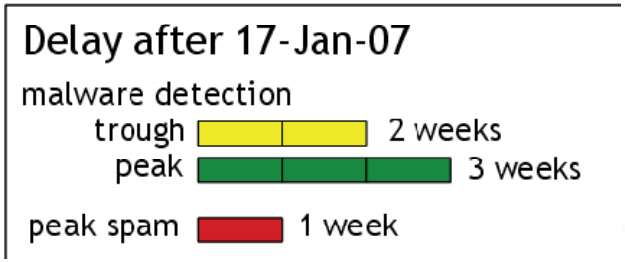
A quantitative assessment of the Storm web threat in 2007

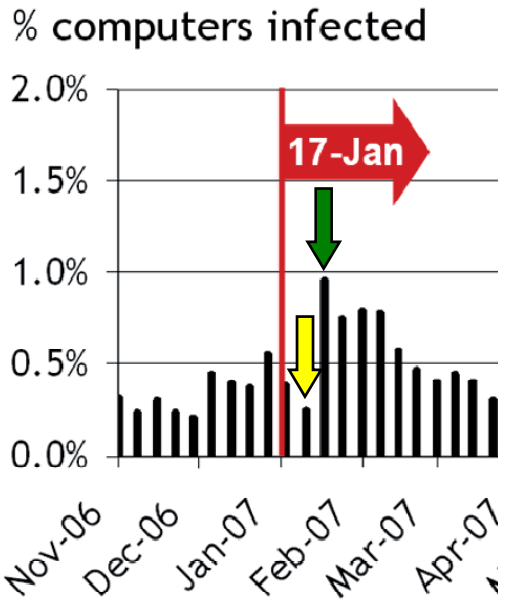


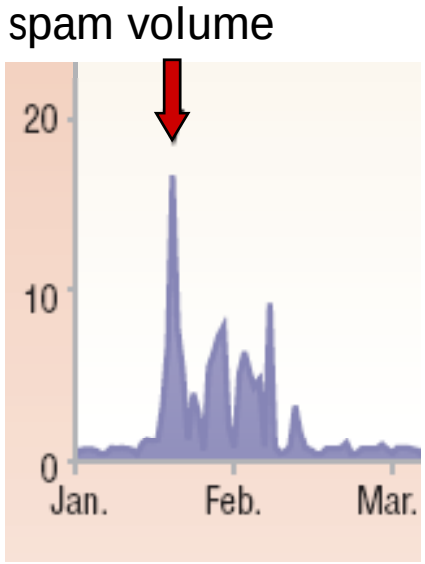
source: Trend Micro

Stormy Weather

A quantitative assessment of the Storm web threat in 2007

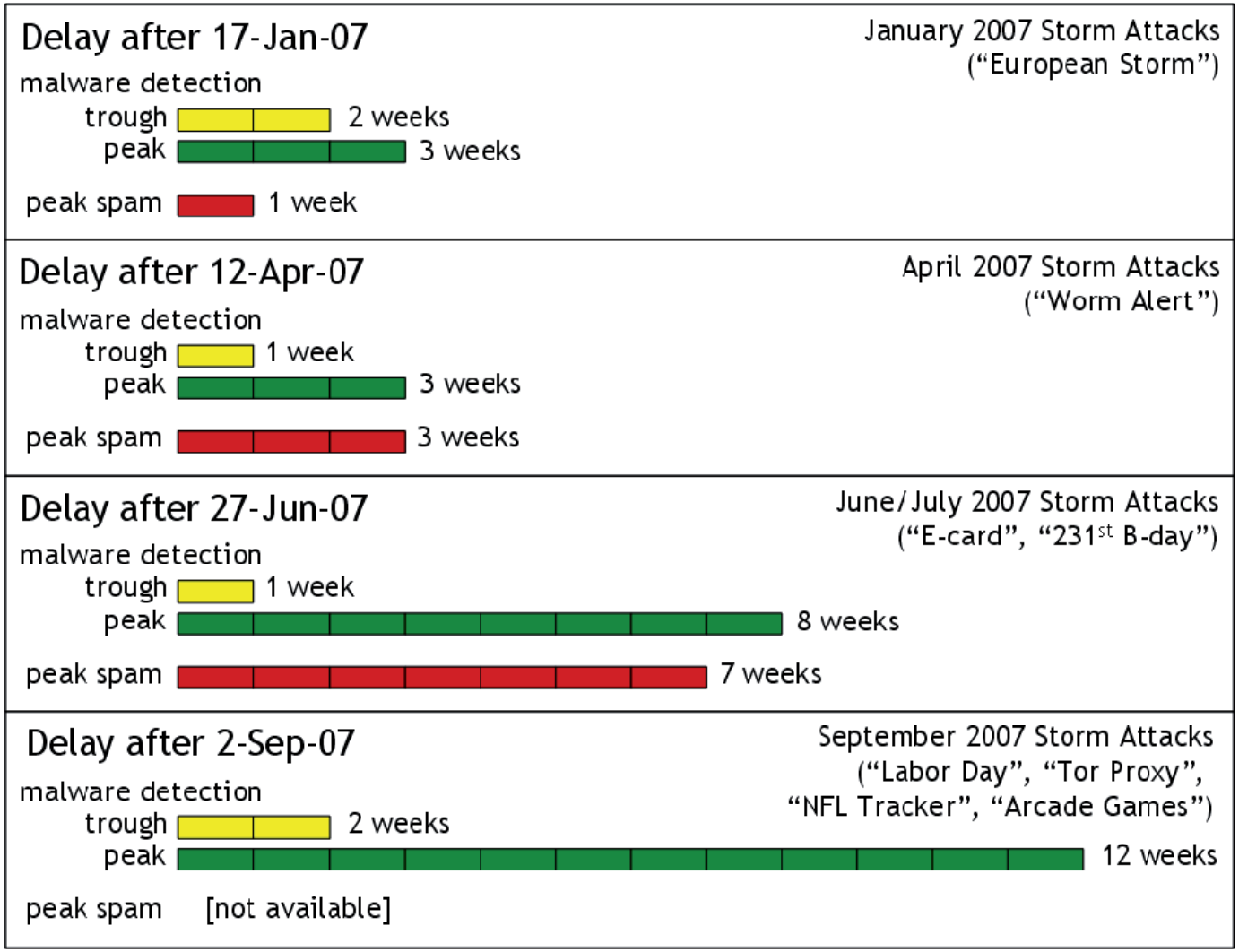






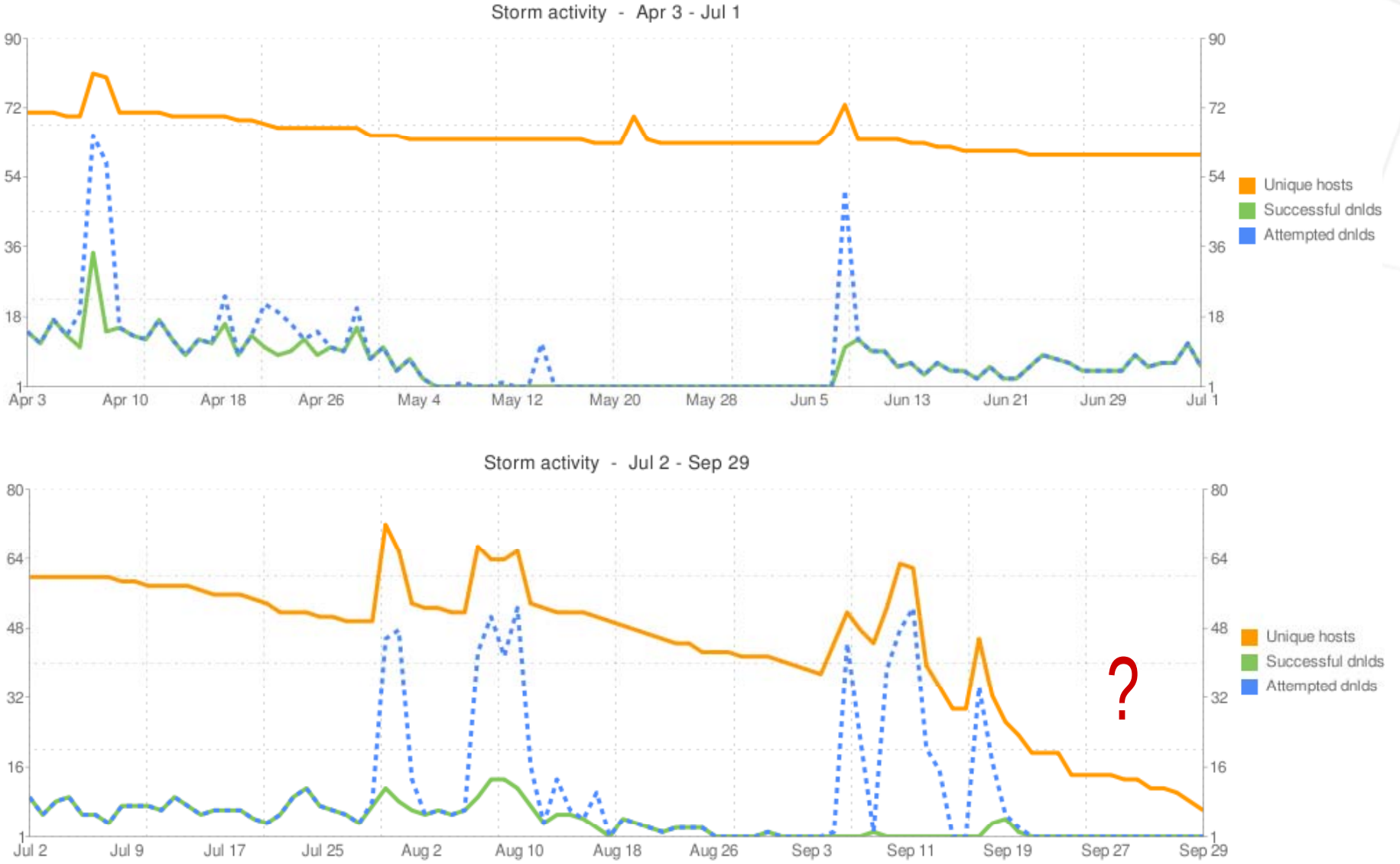
Stormy Weather

A quantitative assessment of the Storm web threat in 2007



Stormy Weather

A quantitative assessment of the Storm web threat in 2007



TREND MICRO

Securing Your Web World

Thank you

VB2008 - Ottawa

October 2008