Mariposa Lessons Learned

David Dagon[1]

with

Chris Davis[2]

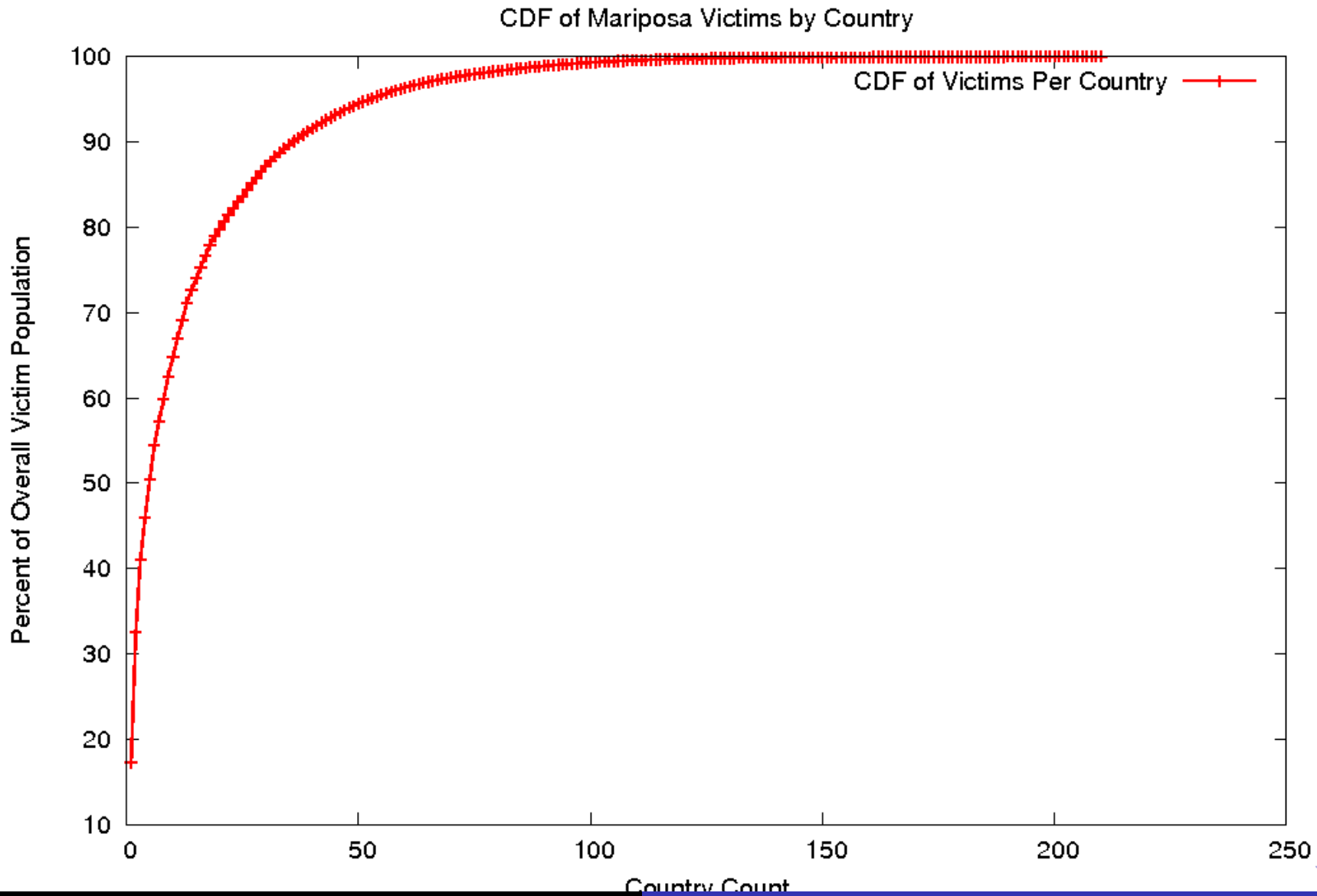
[1]Georgia Institute of Technology, College of Computing
[2]DefIntel, Inc.
dagon@cc.gatech.edu
cdavis@defintel.com

ICANN-37 2010

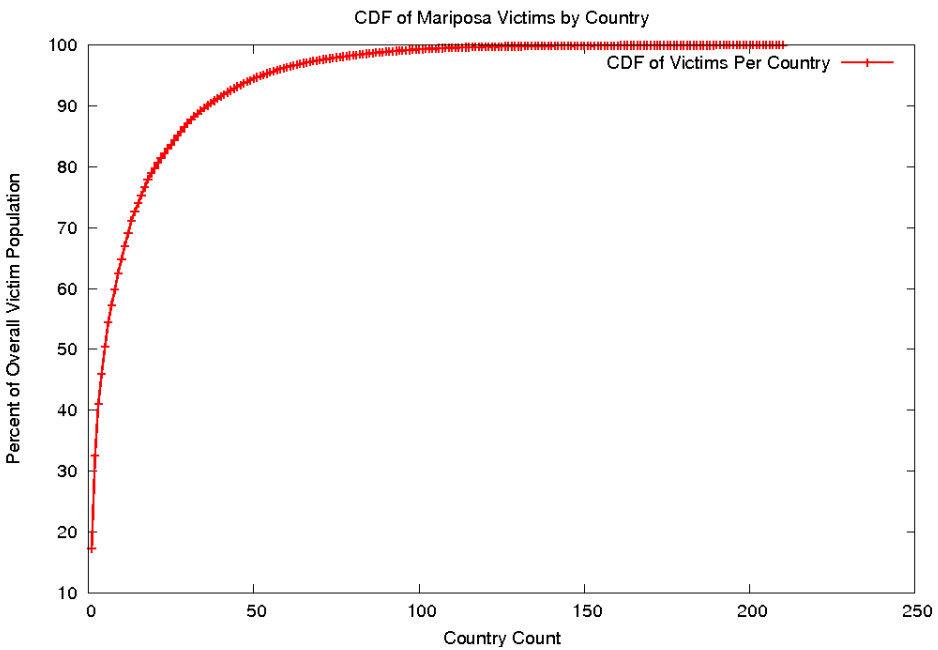
Summary: Lessons from the Mariposa Infection

- Large numbers of victims
- International coordination possible
- Domain “take downs” *do not* stop botnets
  - Botmaster recidivism guaranteed by takedowns
  - Presents mere inconvenience and modest cost to botmasters
- Botnets are international crime scenes and mass invasions of privacy; not marketing/research projects
- Case is ongoing; we present only statistical highlights in deference to the Spanish judicial process

Victim CDF


CDF of Mariposa Victims by Country
CDF of Victims Per Country
Percent of Overall Victim Population
Country Count
100
90
80
70
60
50
40
30
20
10
0
50
100
150
200
250

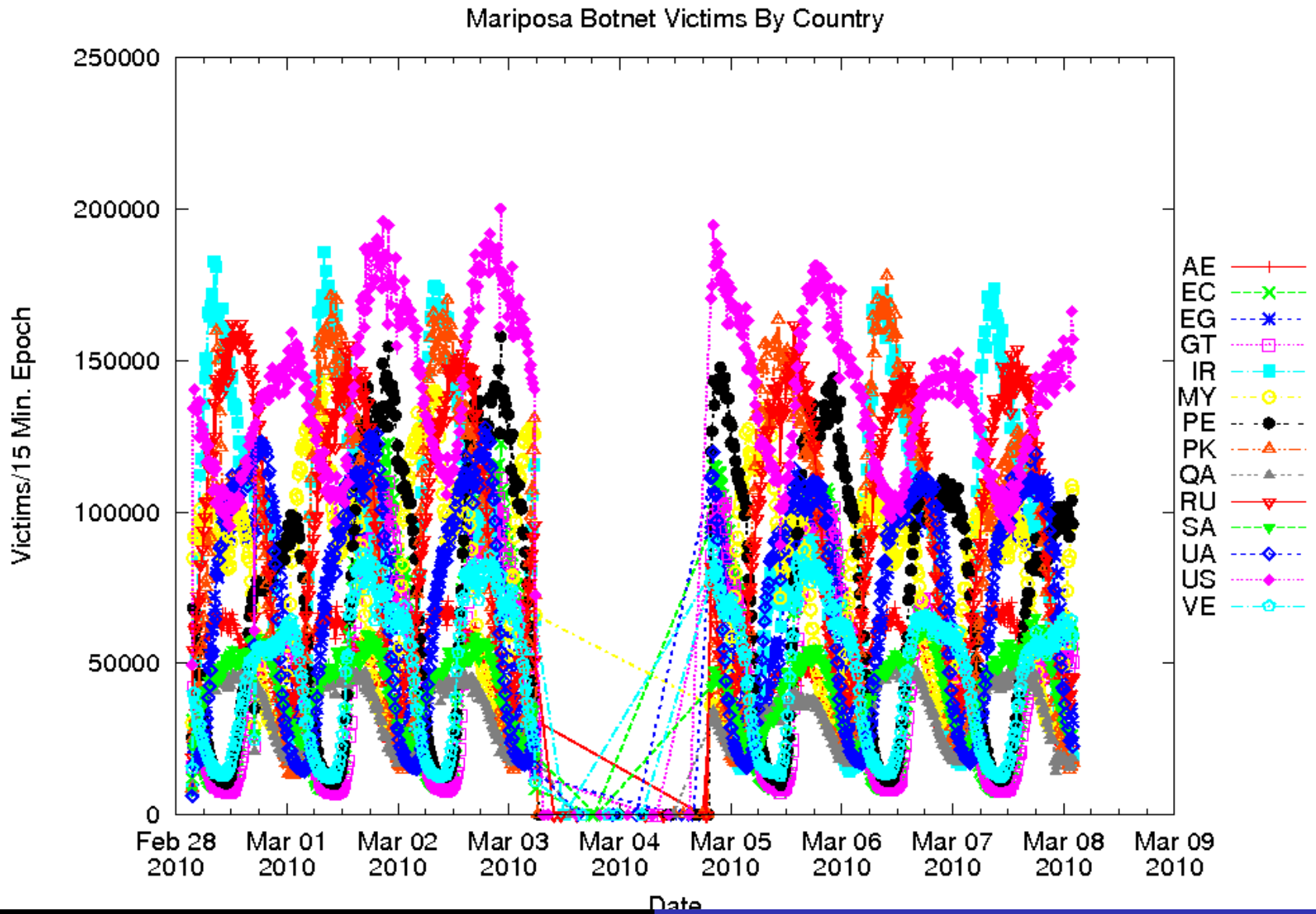
Victim CDF



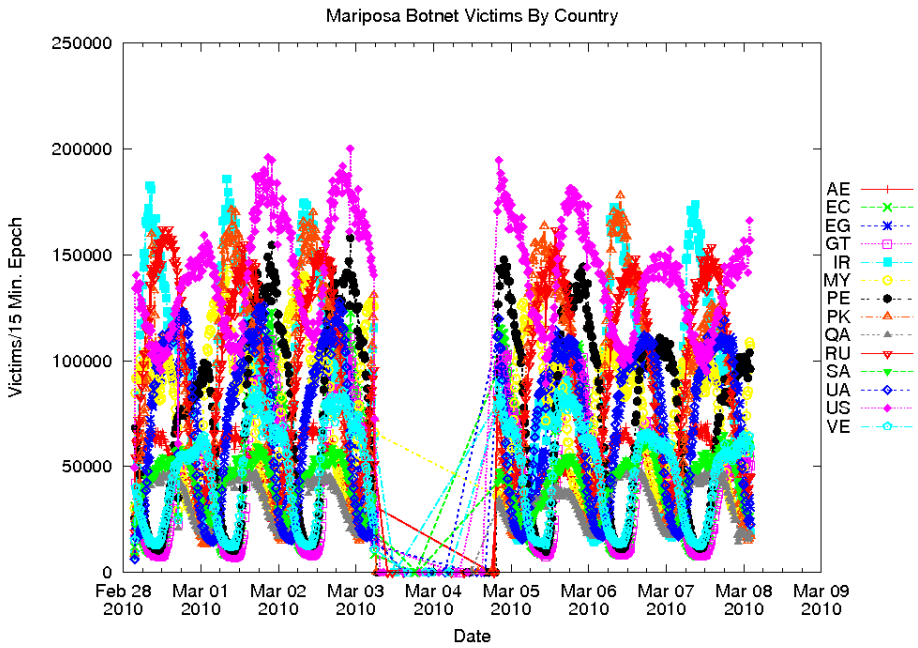
Salient points:

- Enormous spread
- Approx. 50 countries make up 90% of victims
- Mariposa had a broader base of infection by country
  - Not a typical US-focused infection
  - Message-based propagation
  - Rental of botnet may have contributed
- Implication: We all face a common threat

Top Countries Affected by Mariposa



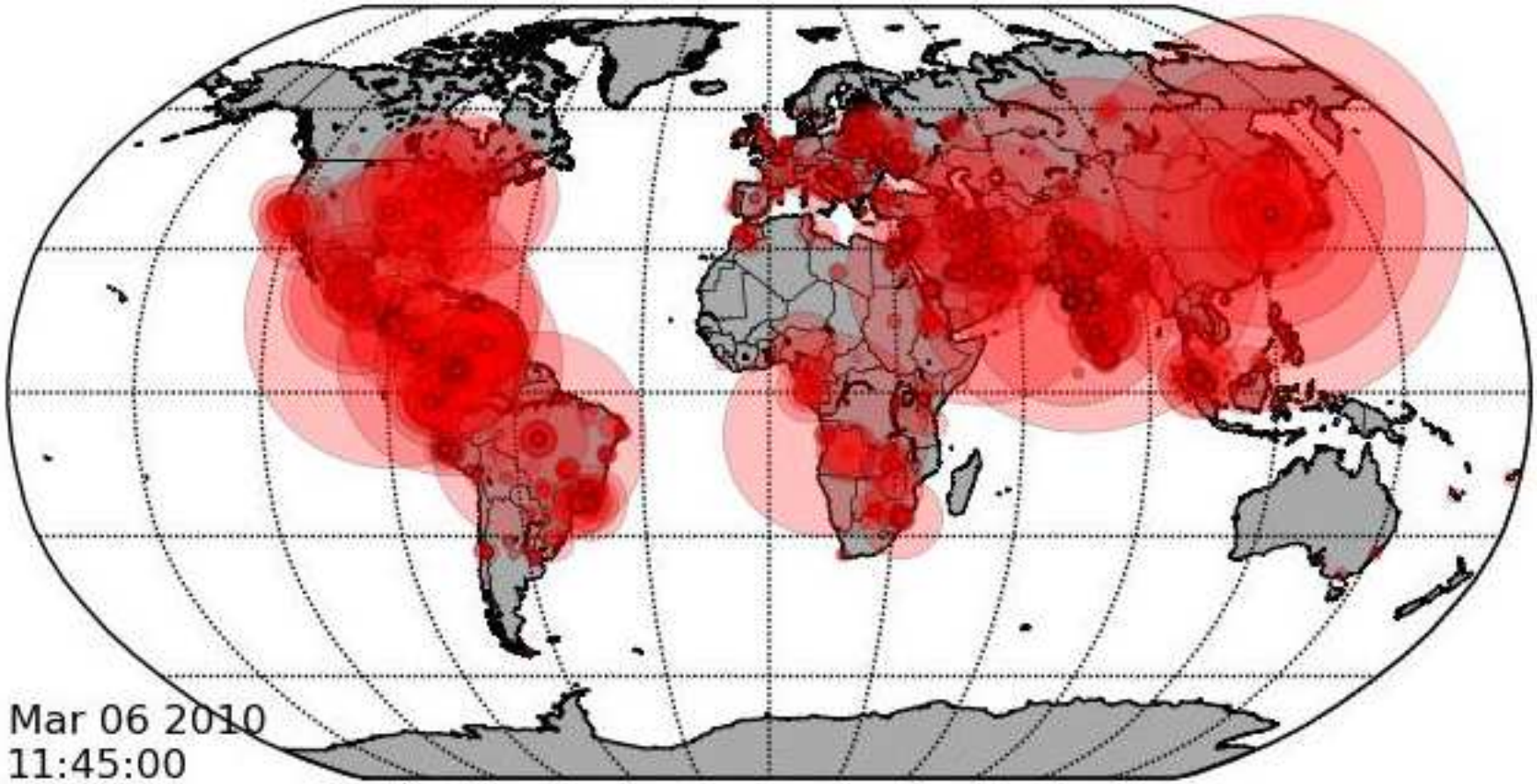
Top Countries Affected by Mariposa



Salient points:

- Brief sensor outage (gap in plot)
- Strongly diurnal patterns for *all*
  - These victims are end users, not servers
- Top countries are not the usual victims

World Victim Distribution



Summary: Lessons from the Mariposa Infection

- Inversion of the popular notions of botnets
  - Common belief: eastern botmasters and western victims
  - Here, botmasters were in Spain and victims were widely distributed
- Implication: We truly face a common threat, not confined in origins to a given geography
- Lessons from the effort:
  - International coordinate very feasible
  - Domain suspension was the most difficult part
    - Suggested standard: indemnification by vetted, bonded researchers *or* court order
    - A standard of “court mandated” remediation would have left this unremediated
- Monitoring for DDNS *strongly* recommended
  - At one point, the case turned on a DNS packet