Infected System (Bot) Metrics
(Problems, Needs & Standards)

Patrick Cain
Resident Research Fellow
APWG
Everybody: ‘We need bot metrics’!

• Bad metrics are as bad as no metrics
  – There is vast over counting
    – One needs to understand ISP IP policy for real measurements
    – Same computer seen at multiple detectors
  • There’s political capital in making bug numbers
  – Everyone uses different definitions

• But what’s in a metric?
  – what are the metrics used for?
  – Capturing the right data via reporting makes metrics are real
    • [use IODEF – we can force certain data in a submission 😊]
What we need in metrics

• They need to be transparent & recyclable
• Not ‘shaming numbers’, deltas, or top 10 lists
• And they will evolve… 😞

• The APWG uses metrics for education & action
  – Crime Fighters never get enough resources
  – How do we show governments/ISPs/ICANN where the problems are?
  – How do we show when the problems get ‘better’
A good use of metrics

• True metrics can be used to enlighten the bosses to direct resources to a problem
  – ex: the APWG phishing report
    • We compile per capita stats on phishing URLs & collectors
    • You could redo our calculations for accuracy
    • People ‘shame’ themselves into corrections

• They also show trends – both upward and downward – and improvements
The needs

• Solid definitions
  – Everyone has to use the same language

• Integrated into or a part of the ISP/end-user reporting and notification systems
  – There needs to more international versions of these

• Ability for independent calculation
  – Not everyone is going to submit raw data.
Thank You

pcain@apwg.org
[Send us data in IODEF.]
[Wait. Send us BOT data in IODEF.]