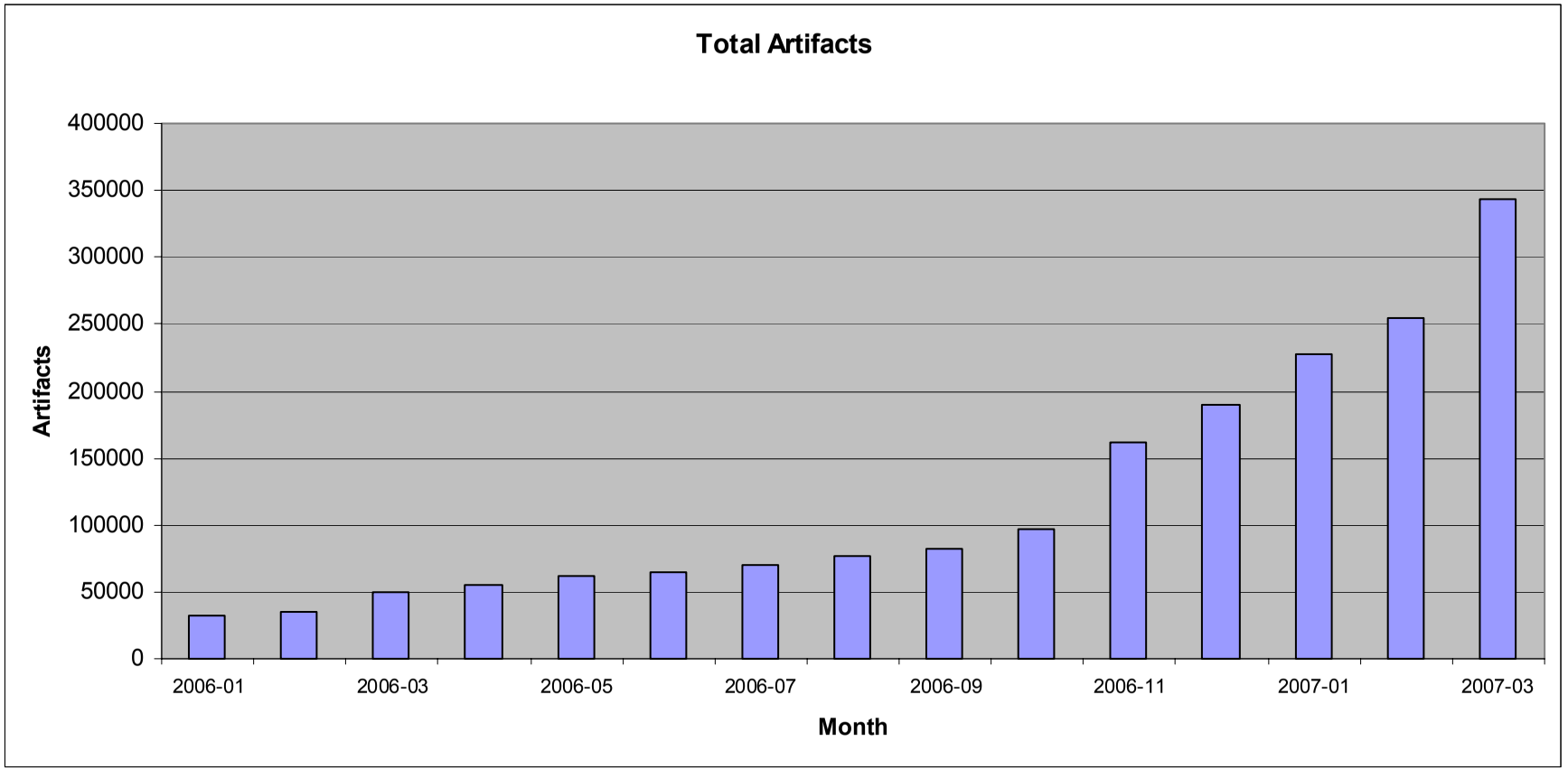
Malcode

APEC/OECD Malware Workshop
APEC-TEL 35

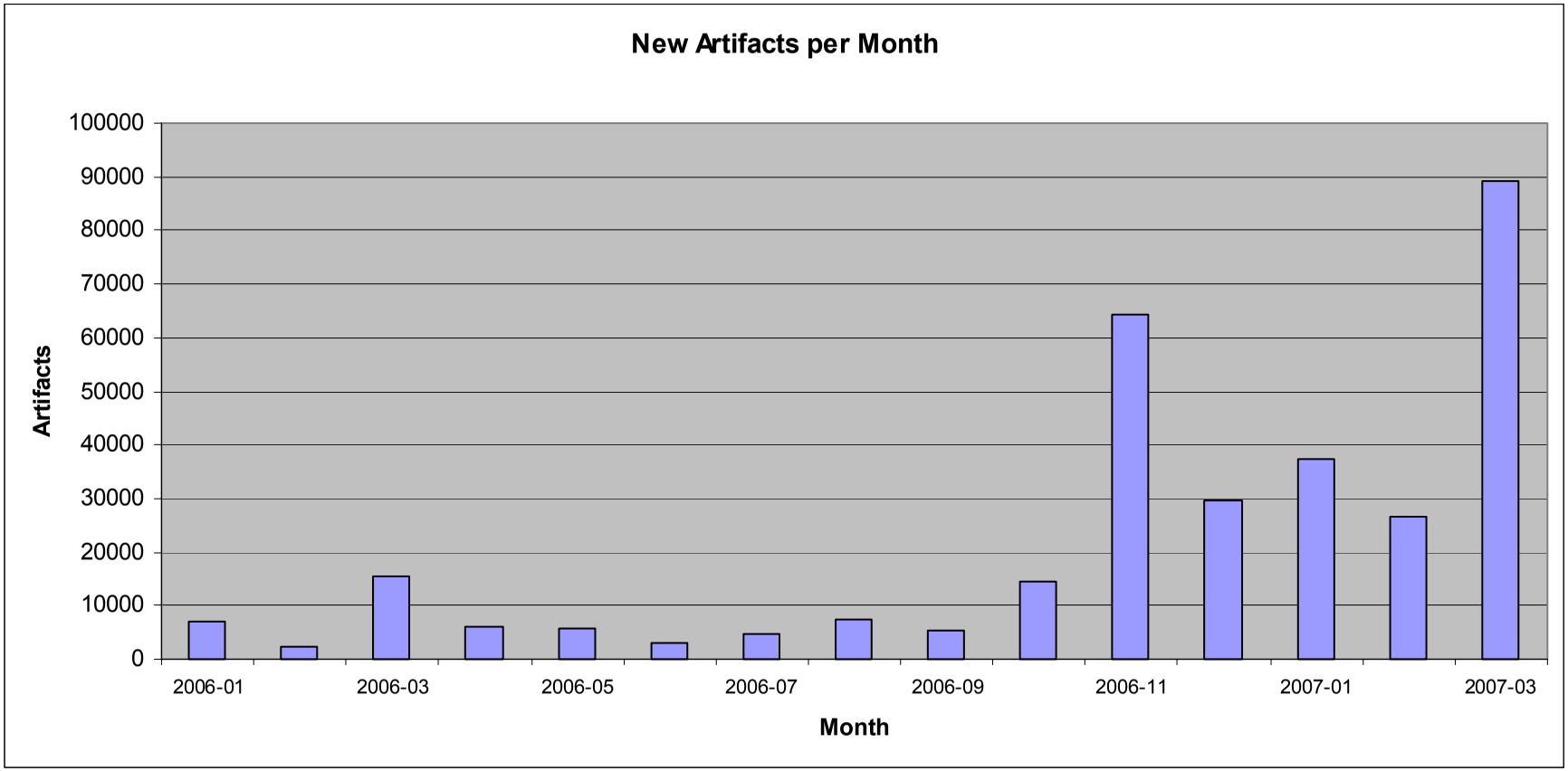
Kevin J. Houle <kjh@cert.org>

22 April 2007

Exponential Growth



Growth Rate by Month



Trends and Challenges

- Attribution; malcode = adversarial tradecraft
- What should we analyze? Impact…
- Time-to-impact; analysis takes time…
- Moving targets and rapid evolution
  - Barriers to technical understanding
  - Characterizations of bad behavior
- Convergence with forensics
- Role of the CSIRT