AusCERT
Australian Computer Emergency Response Team

AusCERT Home Users Computer Security Survey 2008

Kathryn Kerr

Manager, Analysis and Assessments

Agenda

AusCERT
Australian Computer Emergency Response Team

- Scope
- Purpose
- Methodology
- Key findings
- Conclusion

Survey scope

- Random sample of Australian based home computer users with Internet connections
- 18 years +
- 1,001 responses
- conducted March 2008

Purpose

AusCERT
Australian Computer Emergency Response Team

- Threat environment
  - Active targeting of client computers to support variety of cybercrime, including online ID theft
- Seek better understand the security posture, attitudes and awareness of home Internet users in Australia
- Help raise awareness of online security issues among home Internet users

Purpose

- Was there any connection between risky behaviours and incidents of malware infections?
- Some results from the survey support this view but not conclusively

Methodology

- Nielsen, market research and information company
  - Nielsen selected sample, conducted the survey and collated results
  - Nielsen online web portal
  - Results post weighted for age and gender
- AusCERT specified the questions, analysed results and prepared report
- Sample error rate is 3.1%

Malware infections

- 23% reported confirmed malware infections
  - Confirmed means detected by AV or anti-spyware after infection (not quarantined) (15%); or
  - Informed by trusted third party, such as ISP, bank, other professional organisation (11%)
- 70% of these were infected 1+ times in the last 12 months
  - Hence 16% of all respondents had 1 or more confirmed malware infections in last 12 months
    - (70% x 233 = 16% x 1001)

Broadband and malware

AusCERT
Australian Computer Emergency Response Team

- Always on broadband vs connecting computer to broadband only when computer in use.
- 27% of “always on” broadband users (54%) reported malware infections
  - 27% of 540

compared to:

- 14% of broadband users who only connect to the Internet when computer in use (34%) with malware infections
  - 14% of 343

Spam links and malware

- 30% reported clicking on links in spam email
- 32% of this group reported malware infections

compared to:

- 65% said they didn't click on spam email links
- 19% of these reported malware

Disabling security features and malware

AusCERT
Australian Computer Emergency Response Team

- Do you routinely disable AV, firewall or browser security features to allow maximum functionality for online games, P2P etc?
- 13% (132) did sometimes or always disabled security
- 37% of this group reported malware infections

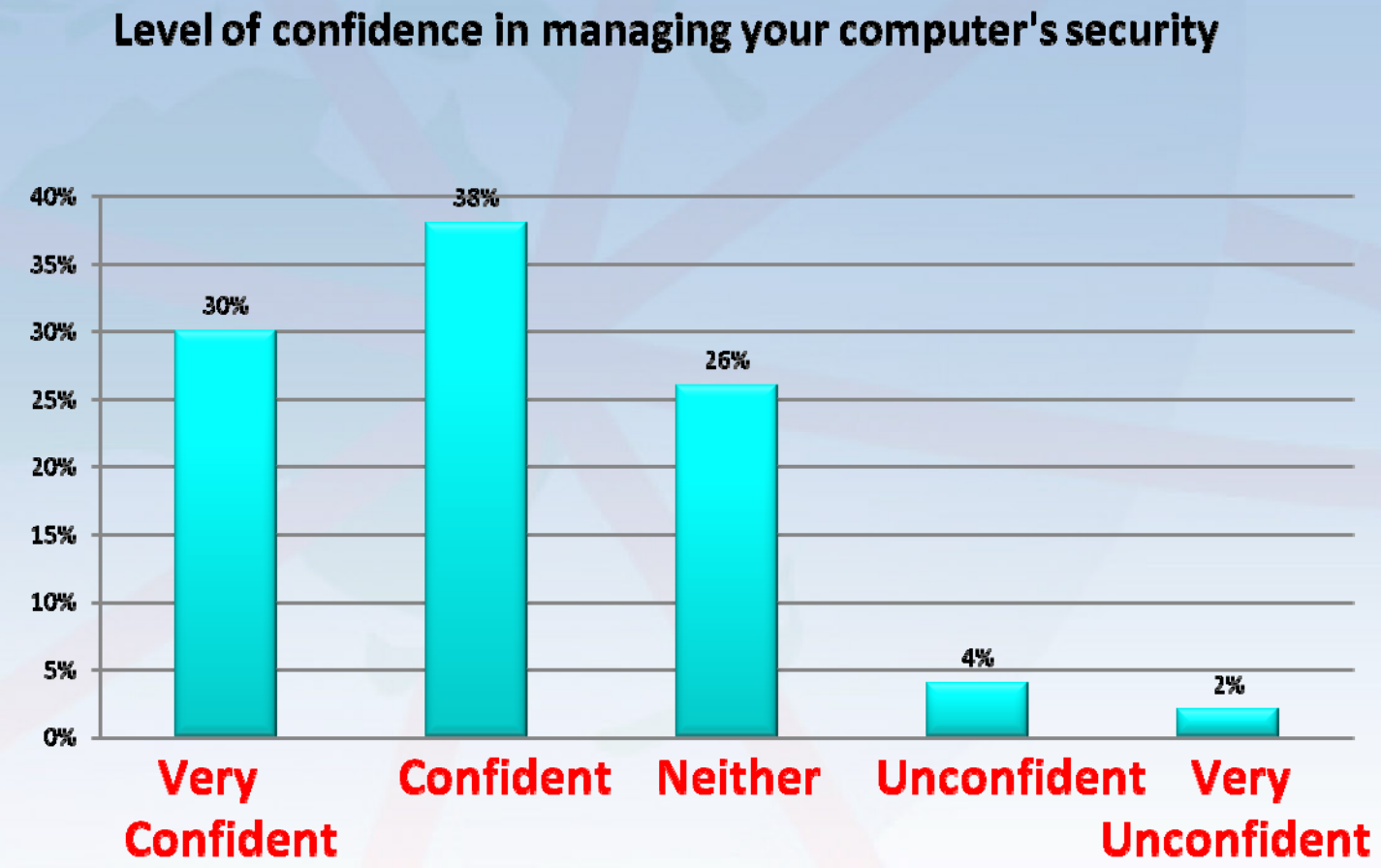
compared to:

- 62% (624) said they never disabled security features
- 21% of these reported malware

Anti-virus software

- 94% have AV software installed
  - But only 70% configure automatic updating for AV "always"
  - 18% only update "sometimes" automatically and 8% "never" update automatically
- 22% with "always" updated AV (70%) still reported malware infections

Confidence vs competence

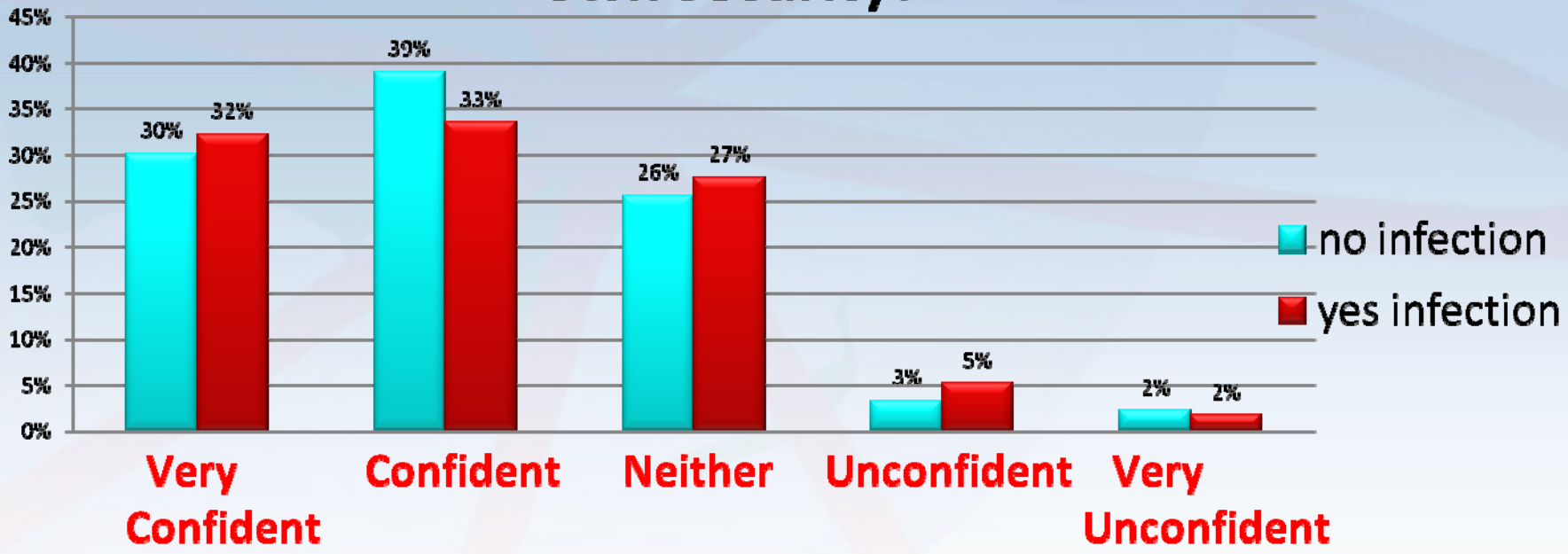


Average confidence level is 7.24, Std. Dev. 2.16
AusCERT User Computer Security Survey 2008, Total respondents 1001, 100%

Confidence vs competence

AusCERT
Australian Computer Emergency Response Team

How confident were those with infections compared to those without to manage their own security?



Total with confirmed infections 233, 23%
Total without infections 768, 77%

Awareness of security issues

AusCERT
Australian Computer Emergency Response Team

- 38% believe they can rely on AV or anti-spyware software to alert them to malware infections
  - Yet we know that approximately 40% of malware not detected on average across vendors* when first found in the wild
  - *Note these figures vary each day and between vendors
- 33% of those who don't use anti-phishing tools (575 or 57%) don't know what a phishing site is

Awareness of security issues

AusCERT
Australian Computer Emergency Response Team

- 46% incorrectly believed that it is not possible for an attacker to see or modify data when SSL is being used
  - which is possible if the computer is compromised with information stealing malware
  - Eg, case study in the report

Summary

AusCERT
Australian Computer Emergency Response Team

- 16% reported malware infections in last 12 months
- Risky online practices were common among home Internet users
  - And result in higher levels of malware infections compared to those who adopt safer online practices
- Over-confidence in abilities, lack of awareness of security issues and poor attitudes to security were present among small proportion of home Internet users
- The report is prepared with a view to help raise awareness among home Internet users of risks and how to best minimise these risks

Get the survey

AusCERT
Australian Computer Emergency Response Team

- Survey is available online from:

http://www.auscert.org.au/usersurvey