AusCERT
Australian Computer Emergency Response Team

ITU Regional Cybersecurity Forum for Asia-Pacific

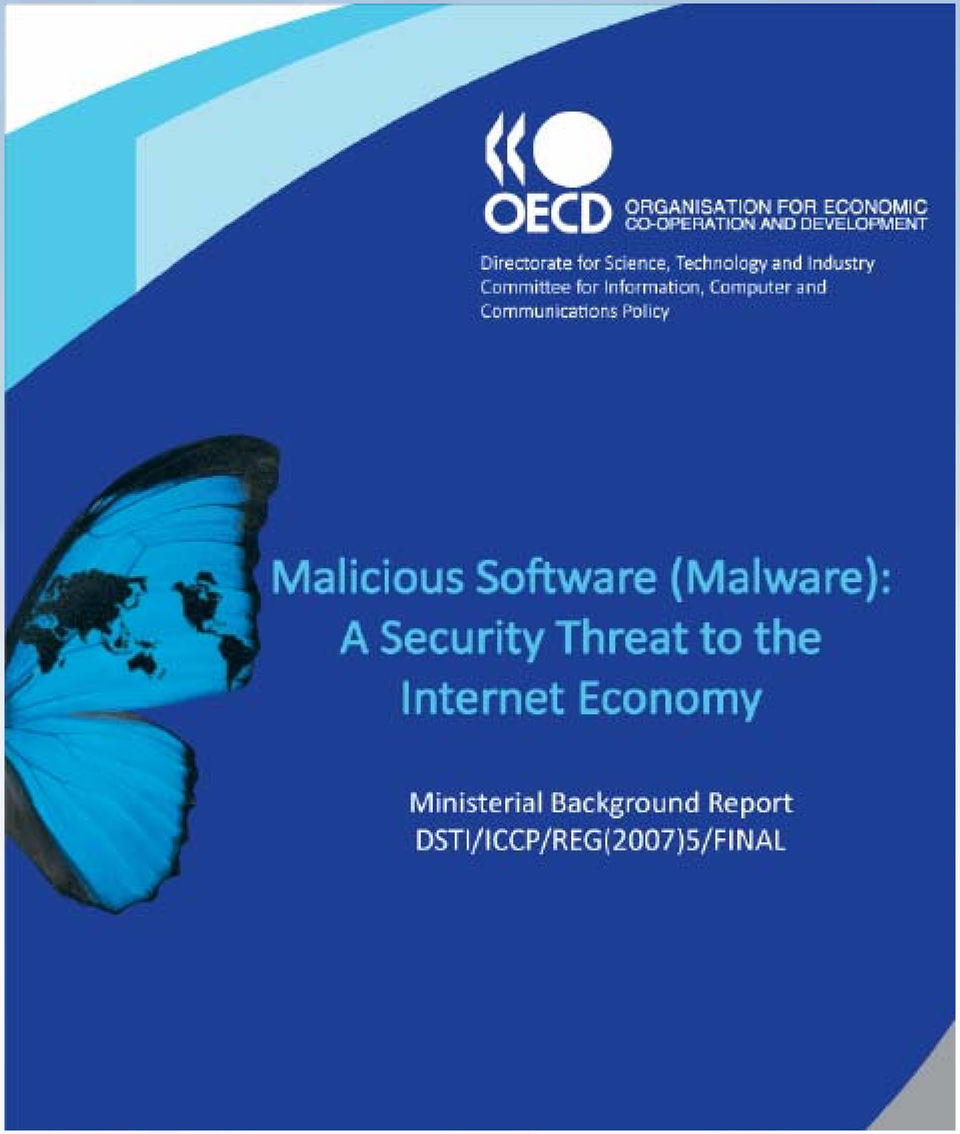
Incident Management Capabilities Australia Country Case Study

Graham Ingram
General Manager AusCERT
July 2008

Responding to Attacks

- The nature of attacks have changed and Incident management/response has also changed
- Nature of attacks:
  - Online identity theft – (still) the number one threat to eGovernment and eBusiness.
  - Attacks on availability – a close second…
  - State sponsored attacks and Terrorism

The lines are blurred



OECD ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Directorate for Science, Technology and Industry
Committee for Information, Computer and Communications Policy

Malicious Software (Malware): A Security Threat to the Internet Economy

Ministerial Background Report
DSTI/ICCP/REG(2007)5/FINAL

OECD

- A strategy for a global partnership against malware is needed to avoid it becoming a **serious threat to the Internet economy** and to **national security** in the coming years. Today, communities involved in fighting malware offer essentially a fragmented local response to a global threat.
- Malicious software, commonly known as “malware”, is software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners. Over the last 20 years, malware has evolved from occasional “exploits” to a **global multi-million dollar criminal industry**.

Technology Drivers

AusCERT
Australian Computer Emergency Response Team

- Social Networking
  - MSN
  - Facebook
  - Myspace
  - Secondlife
- P2P Networking
- Web 2.0
- Web Apps
- NGN
- Mobile Devices

National CERT Fire Brigade

AusCERT
Australian Computer Emergency Response Team

What is AusCERT doing?

- Monitoring and providing advice about threats and vulnerabilities
- Incident response and mitigation assistance for ongoing attacks
- Performing analysis of attacks and malware to understand the nature of the threat
- Central coordination and collation for data in order to develop metrics on how the threat is changing

Risk Management Stages

Intelligence

Used to inform all stages of the response chain by providing assessments of threats and vulnerabilities

Deterrence	Prevention	Detection	Response	Recovery
A deterrence posture makes the attacker perceive the rewards as low and risks too high	Preventative controls seek to minimise risk from vulnerabilities and exploitation	Detection works where prevention has failed. Early detection of high risk events minimises risk	Detection has to be backed up by rapid response and mitigation	Recovery seeks to minimise fraud risk and repair damage when previous steps have failed

Challenges for managing e-Security risks

- Low visibility of attackers, their tools, techniques, organisation & communications, end-to-end attack and response process
- Attacks can be difficult to detect, track and respond to
- Users can have little knowledge of how compromises took place and are often unwilling to confess to having disclosed information or infection
- Difficult to get comprehensive view of threats and impact of attacks across the enterprise
- Limited progress made in intelligence gathering and sharing with law enforcement
- Incident management is time consuming, isn't core business & requires specialist skills

Incident response

- To provide active support and reduce the impact for organisations and individuals who could not by themselves mitigate an attack or reduce their risk.
- Focuses on what is happening technically
  - how to stop the incident often in real time
  - What hosts (IP address) and domains are involved
  - What is the technical functionality of the attack
  - how to prevent it.
- Working with others
  - Knowing who to contact
  - Whether they can assist
  - Having trust and credibility
  - Getting them to assist

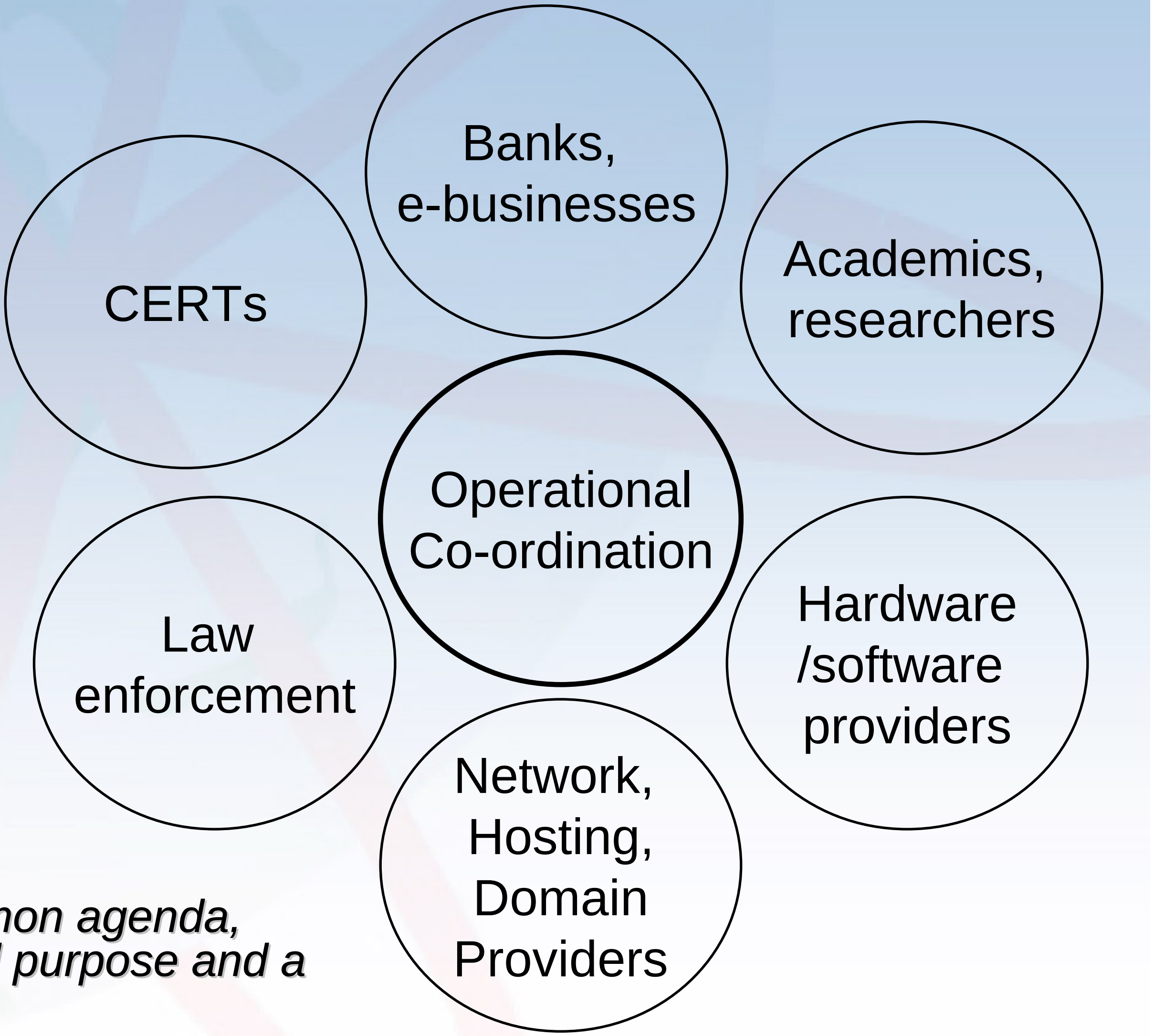
Incident response

AusCERT
Australian Computer Emergency Response Team

- Agreed systematic handling procedures
  - timely
  - secure (eg, encryption)
  - standardised and documented, eg,
  - Consistent data acquisition and recovery forensically sound (if possible)
- Automated system monitoring and analysis tools
  - For dealing with large volumes of complex incidents
  - For automating incident response
  - For generating reports of incidents and incident status
  - Monitoring up and down times
  - Consistent methodology over time
  - Reduces duplication and improves timeliness and efficiencies
- Centralised data collection and submission
  - Eg malware submission
  - Standardised incident reports (eg structured web data)

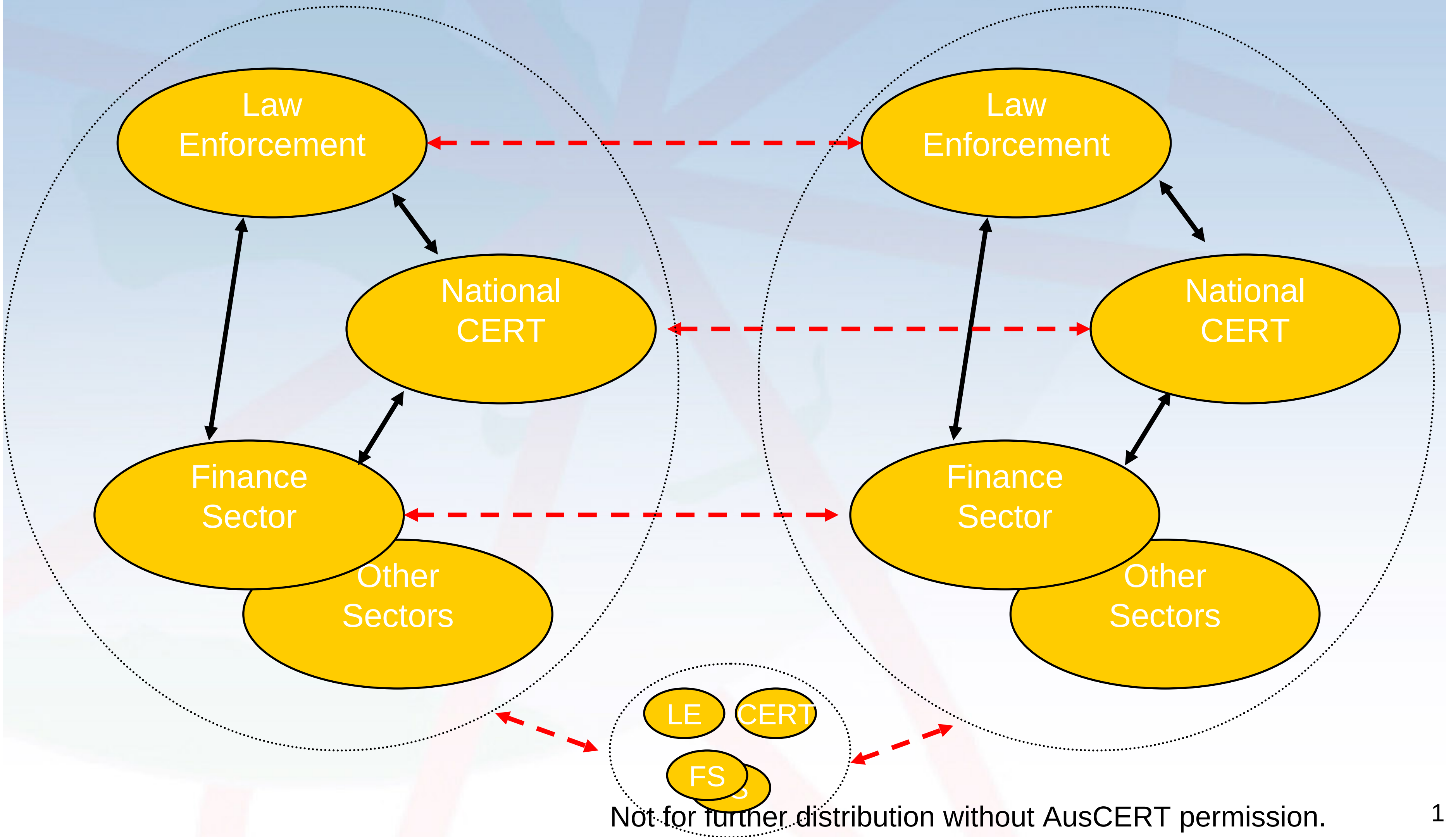
Co-operative Response Structures

- Co-ordination
- Threat data repository
- Threat analysis
- Incident response
- Passive DNS
- Trend analysis
- Metrics
- Intelligence development


CERTs
Banks, e-businesses
Academics, researchers
Operational Co-ordination
Law enforcement
Hardware /software providers
Network, Hosting, Domain Providers

But all parties must have a common agenda, methods and concepts, a shared purpose and a desire for the same outcome

Model for Domestic and International Co-ordination

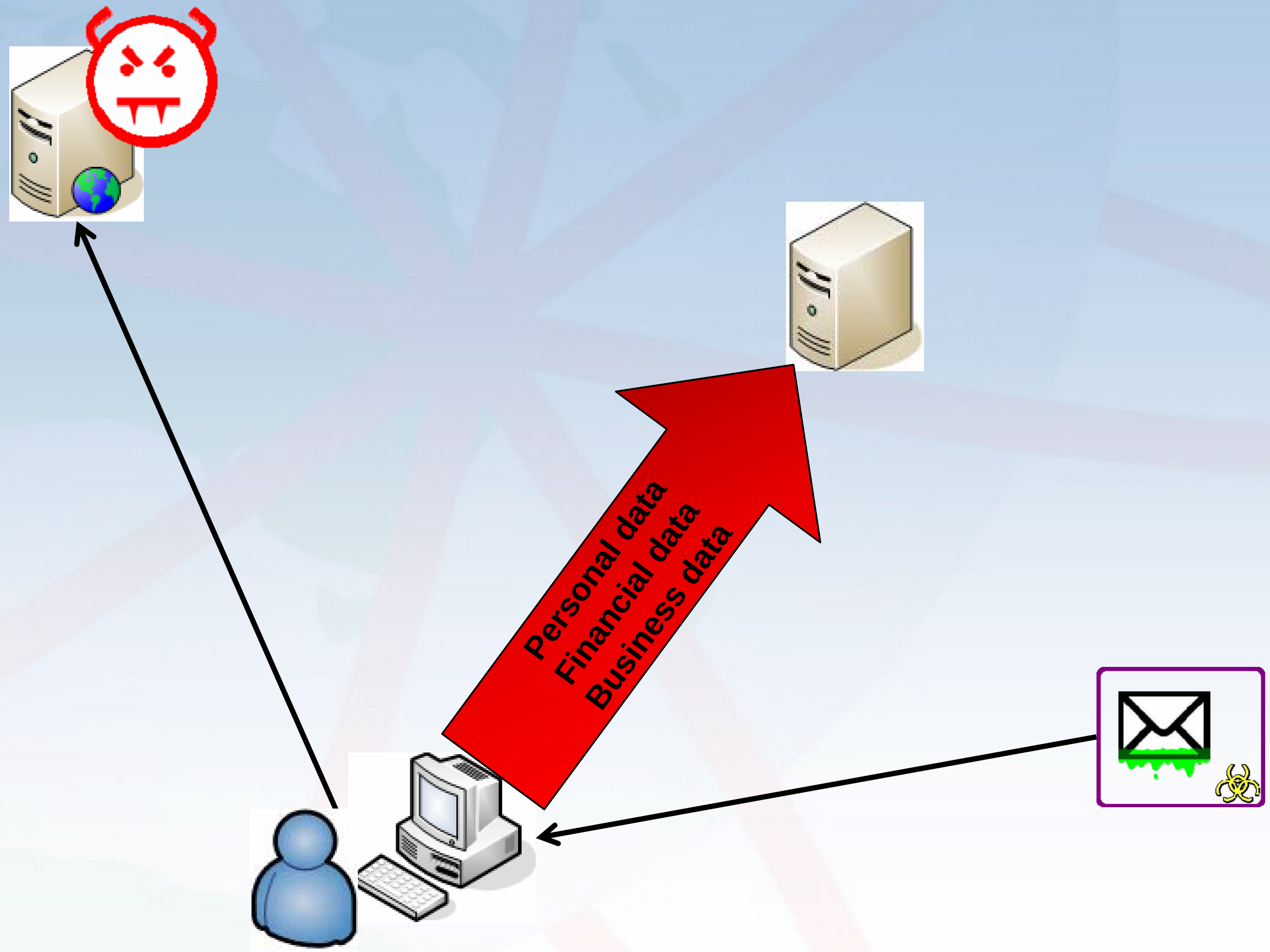


Key requirements

AusCERT
Australian Computer Emergency Response Team

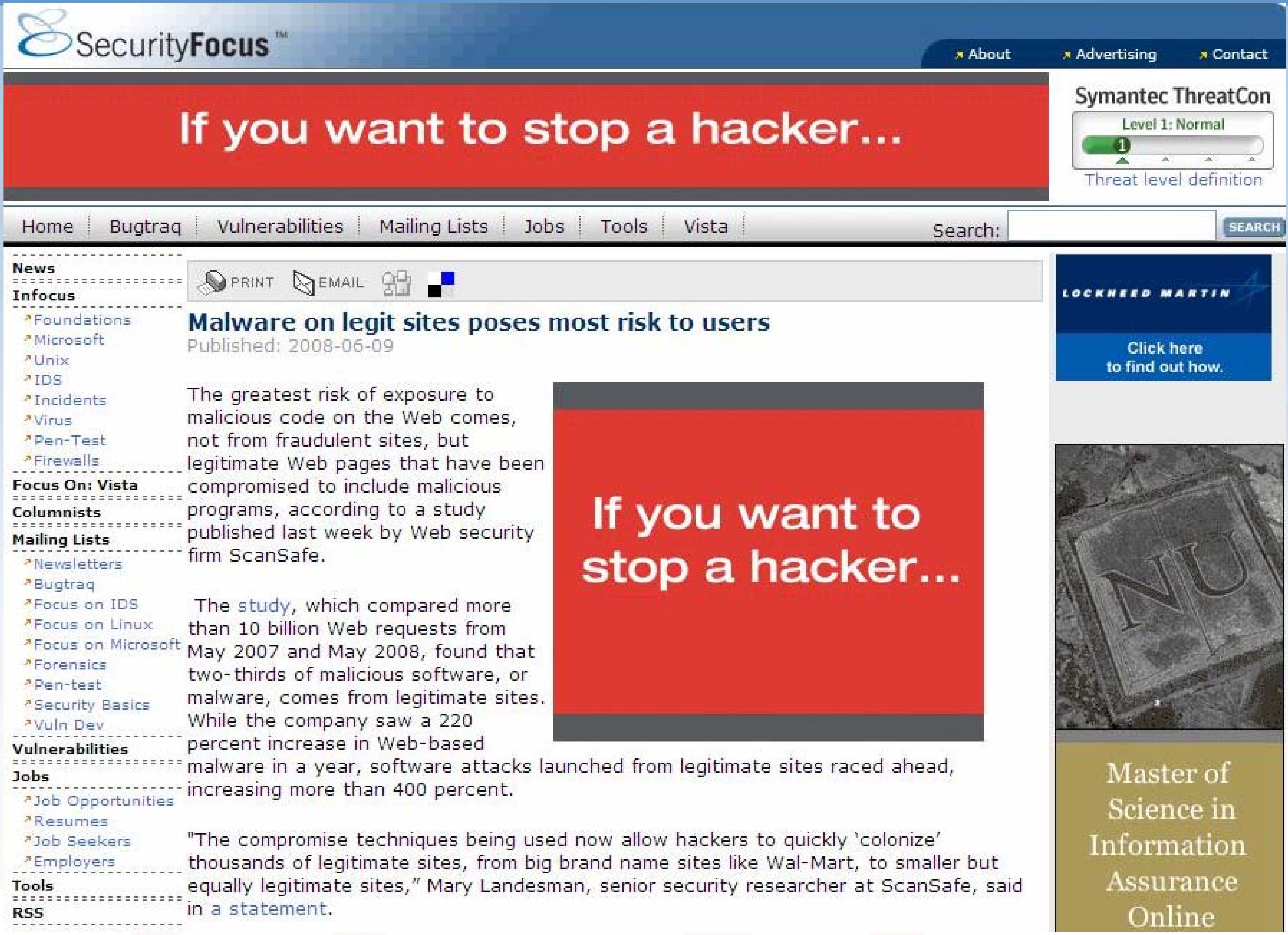
- Better detection mechanisms to identify and track attacks
- Shared knowledge of attack methodologies and trends
- Rapid cross border incident response
- Better understanding of mitigation approaches
- Better access to quality data for analysis and assessments
- Capacity to deal with CERTs, industry (including vendors and ISPs), government and law enforcement

generic_picture_here



Web app vulnerabilties

- The one class of server-side vulnerability that is still a hot favourite
- Largest volume attacks involve off-the-shelf PHP web applications
- Rather than scanning, specific vulnerabilities are searched for (e.g. using Google) then exploited
  - Attack often automated – bulk compromises
- Consequently, many cyber attacks are hosted on legitimate but compromised web sites.



Malware on legit sites poses most risk to users

Published: 2008-06-09

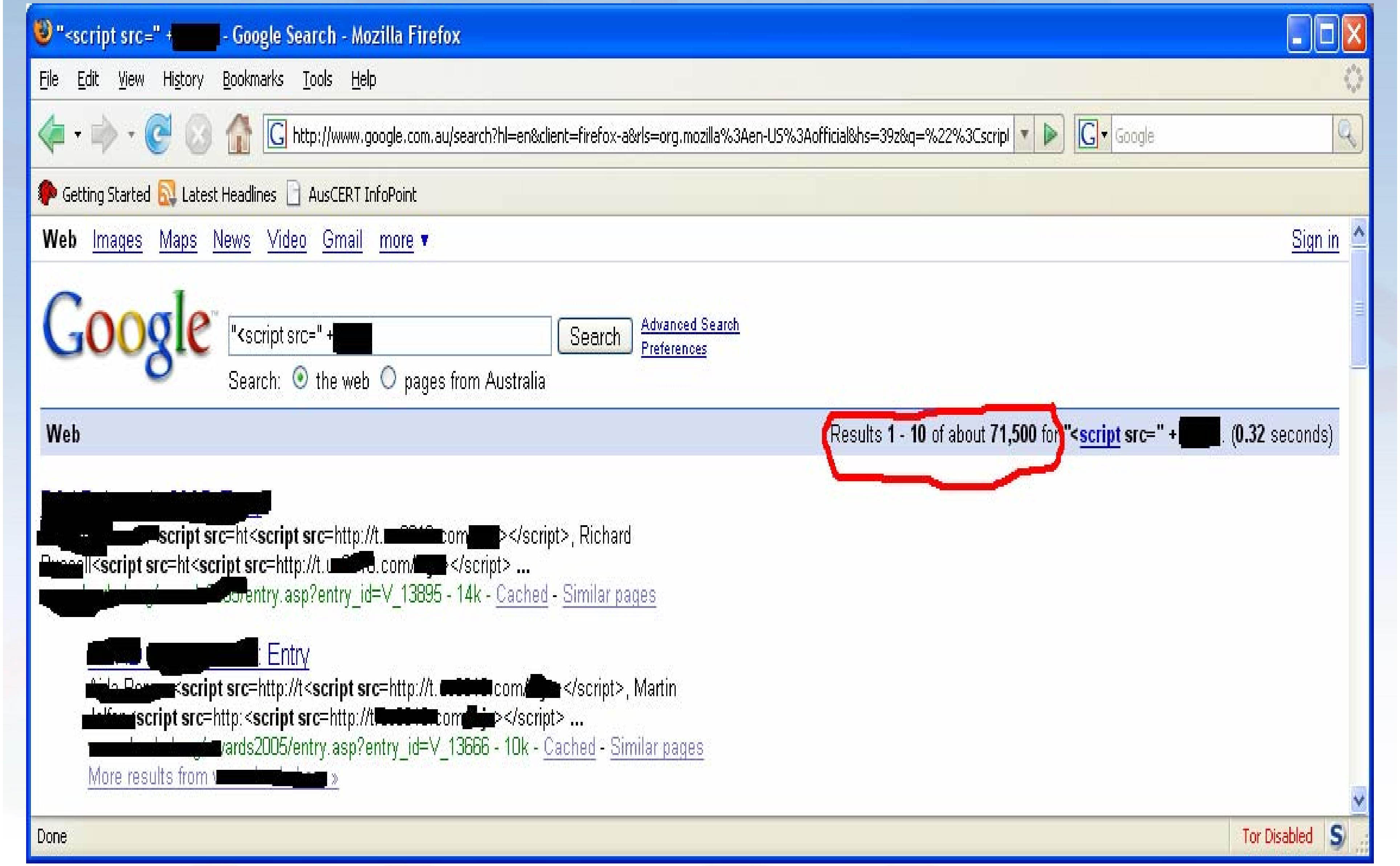
The greatest risk of exposure to malicious code on the Web comes, not from fraudulent sites, but legitimate Web pages that have been compromised to include malicious programs, according to a study published last week by Web security firm ScanSafe.

The study, which compared more than 10 billion Web requests from May 2007 and May 2008, found that two-thirds of malicious software, or malware, comes from legitimate sites. While the company saw a 220 percent increase in Web-based malware in a year, software attacks launched from legitimate sites raced ahead, increasing more than 400 percent.

"The compromise techniques being used now allow hackers to quickly 'colonize' thousands of legitimate sites, from big brand name sites like Wal-Mart, to smaller but equally legitimate sites," Mary Landesman, senior security researcher at ScanSafe, said in a statement.

On the web

AusCERT
Australian Computer Emergency Response Team



"<script src=" + [redacted] - Google Search - Mozilla Firefox

http://www.google.com.au/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=39z&q=%22%3Cscript

"<script src=" + [redacted]

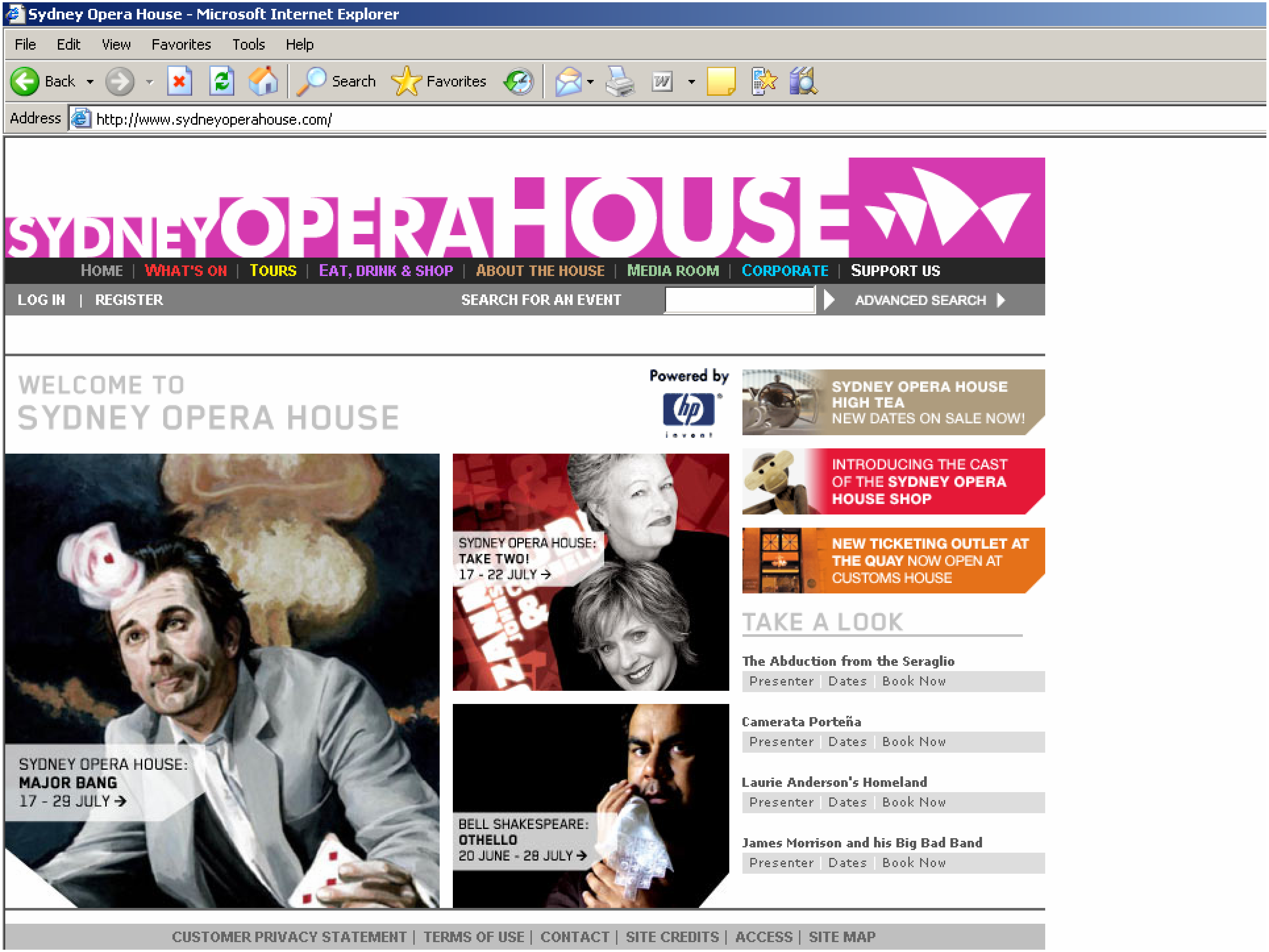
Search: ● the web ○ pages from Australia

Web Results **1** - **10** of about **71,500** for **"<script src=" +** [redacted]. (**0.32** seconds)

[redacted]

[redacted] **script src=**ht<**script src=**http://t.[redacted]com[redacted]></script>, Richard [redacted]ll<**script src=**ht<**script src=**http://t.[redacted].com/[redacted]</script> **...**
[redacted]entry.asp?entry_id=V_13895 - 14k - Cached - Similar pages

[redacted] Entry
[redacted]<**script src=**http://t<**script src=**http://t.[redacted]com/[redacted]</script>, Martin [redacted]**script src=**http:<**script src=**http://t[redacted]com[redacted]></script> **...**
[redacted]ards2005/entry.asp?entry_id=V_13666 - 10k - Cached - Similar pages
More results from [redacted] »


Sydney Opera House - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://www.sydneyoperahouse.com/

SYDNEY OPERA HOUSE

HOME | WHAT'S ON | TOURS | EAT, DRINK & SHOP | ABOUT THE HOUSE | MEDIA ROOM | CORPORATE | SUPPORT US

LOG IN | REGISTER SEARCH FOR AN EVENT ADVANCED SEARCH

WELCOME TO
SYDNEY OPERA HOUSE

Powered by hp invent

SYDNEY OPERA HOUSE:
MAJOR BANG
17 - 29 JULY →

SYDNEY OPERA HOUSE:
TAKE TWO!
17 - 22 JULY →

BELL SHAKESPEARE:
OTHELLO
20 JUNE - 28 JULY →

SYDNEY OPERA HOUSE HIGH TEA
NEW DATES ON SALE NOW!

INTRODUCING THE CAST OF THE **SYDNEY OPERA HOUSE SHOP**

NEW TICKETING OUTLET AT THE QUAY NOW OPEN AT CUSTOMS HOUSE

TAKE A LOOK

The Abduction from the Seraglio
Presenter | Dates | Book Now

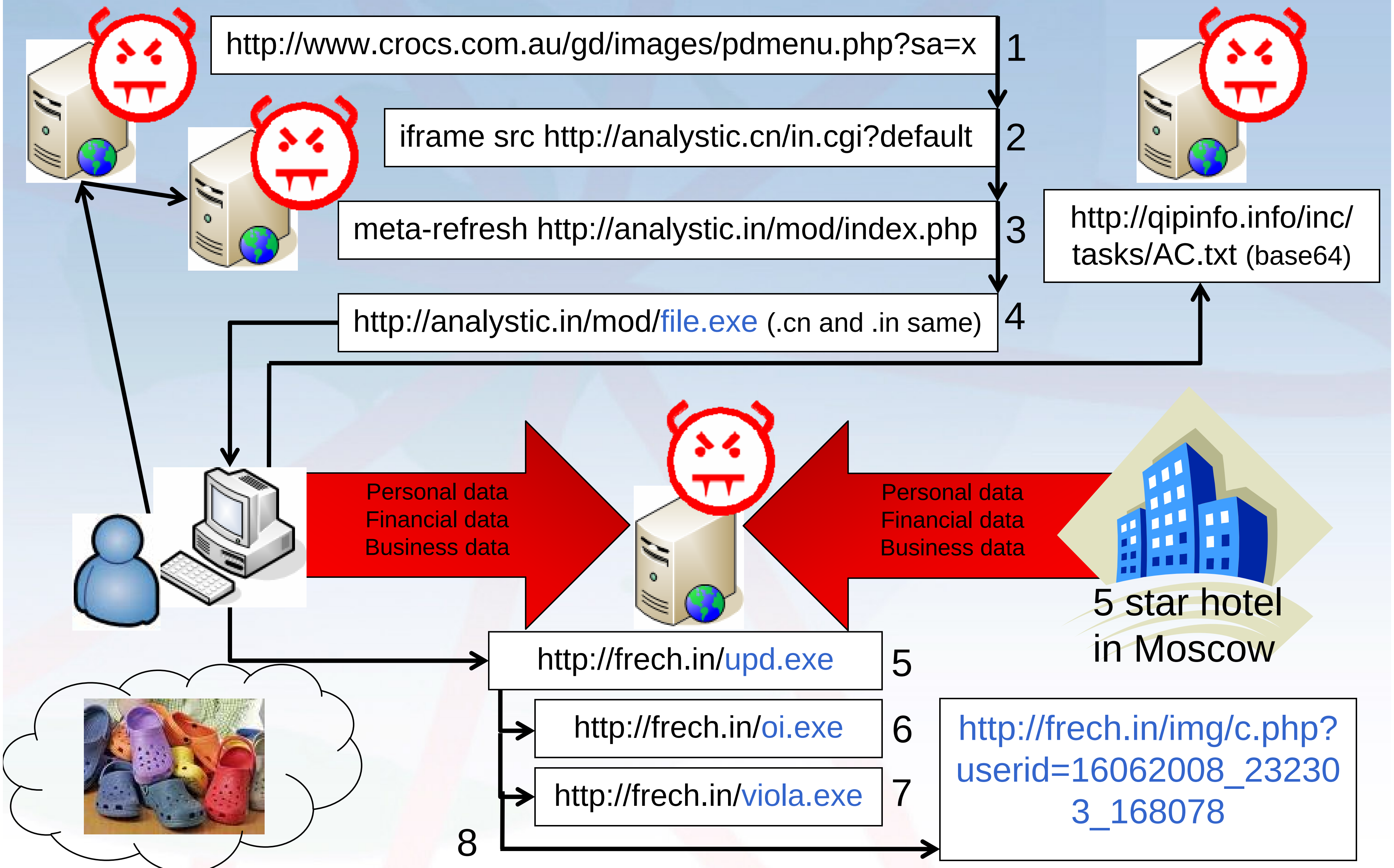
Camerata Porteña
Presenter | Dates | Book Now

Laurie Anderson's Homeland
Presenter | Dates | Book Now

James Morrison and his Big Bad Band
Presenter | Dates | Book Now

CUSTOMER PRIVACY STATEMENT | TERMS OF USE | CONTACT | SITE CREDITS | ACCESS | SITE MAP

Crocs Case Study



1 http://www.crocs.com.au/gd/images/pdmenu.php?sa=x

2 iframe src http://analystic.cn/in.cgi?default

3 meta-refresh http://analystic.in/mod/index.php

4 http://analystic.in/mod/file.exe (.cn and .in same)

http://qipinfo.info/inc/tasks/AC.txt (base64)

Personal data
Financial data
Business data

Personal data
Financial data
Business data

5 star hotel in Moscow

5 http://frech.in/upd.exe

6 http://frech.in/oi.exe

7 http://frech.in/viola.exe

8

10 http://frech.in/img/c.php?userid=16062008_232303_168078

Response

Require initiatives that will improve cyber security and prevent and mitigate impact of cyber crime nationally and internationally, eg

- Improved detection and analysis methods and systems
- improved fraudulent domain deregistration procedures and timeliness
- Improved procedures for closure of bots (compromised machines being used to support cyber crime)
- Improved quality of security advice and awareness initiatives
- Need for better understanding of the nature of the cyber threats and vulnerabilities by those assessing risk

AusCERT
Australian Computer Emergency Response Team

Thank you.

www.auscert.org.au
auscert@auscert.org.au