AusCERT
Australian Computer Emergency Response Team

# Responding to a Denial of Service Attack

Joel Hatton

AusCERT was Australia's first national CERT

- AusCERT is one of the oldest CERTs in the world
- *CERT Australia* is now the National CERT

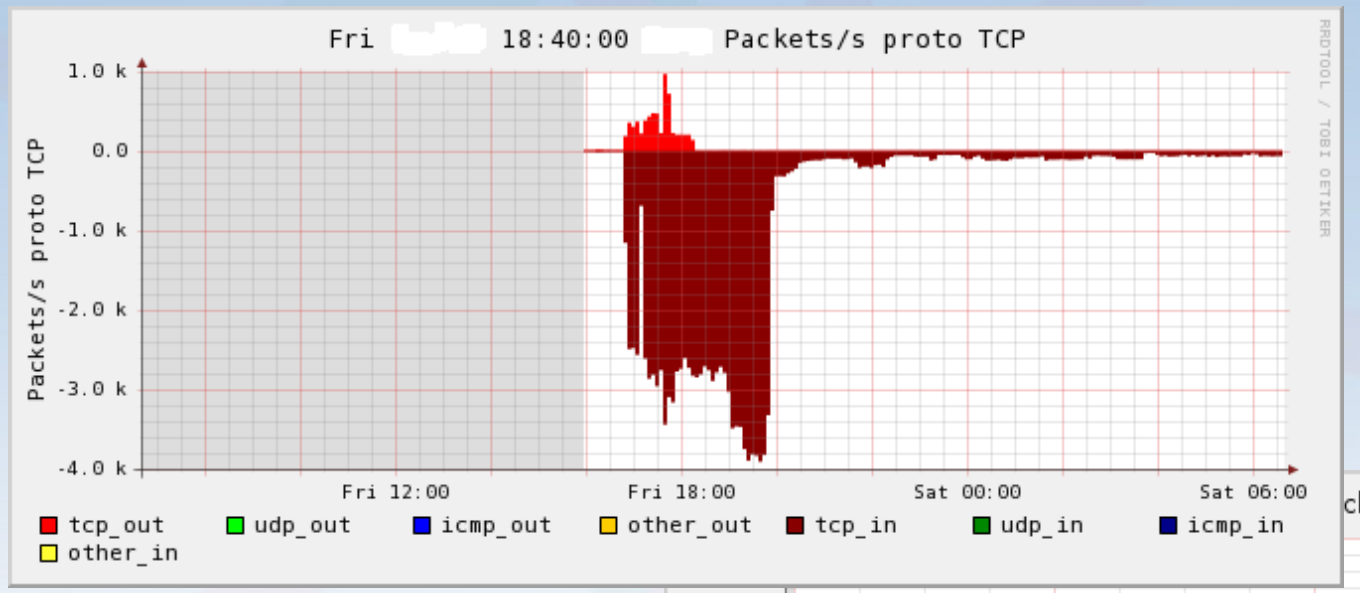
AusCERT is independent and impartial

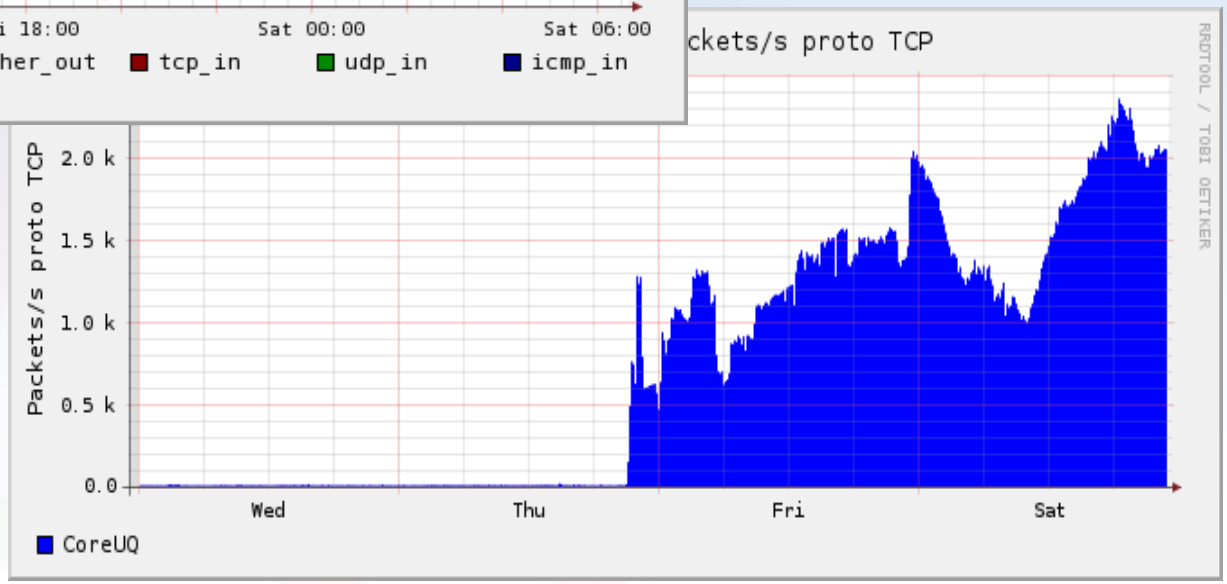
- University-based, non-government, non-profit
- Government, education and business subscribes to AusCERT services

The impact on a networked society can be severe; a **DDoS** attack can disrupt an entire economy...


Image courtesy of the University of Texas Libraries,
The University of Texas at Austin.

# AusCERT targeted...



Develop standard operating procedures

Keep an up-to-date contact list

Understand your ‘normal’

# *is it an attack?*

AusCERT
Australian Computer Emergency Response Team

... not a mis-configuration or power outage

... not the ‘Slashdot Effect’ or self-promotion

So... what type of attack is it?

AusCERT
Australian Computer Emergency Response Team

Follow the plan you developed earlier

Begin recording your actions

Communicate...

# *phased mitigation*

AusCERT
Australian Computer Emergency Response Team

Implement upgrades or workarounds

Look for patterns

Switch over to standby systems

Disable services

# *seeking assistance*

AusCERT
Australian Computer Emergency Response Team

...your up-stream provider

...your peer organisations

...CERTs



Logging can be overwhelmed

Other services may be targeted

Disabled services don’t produce logs



Inform any involved parties

Reverse any configuration changes

Review and lessons learned

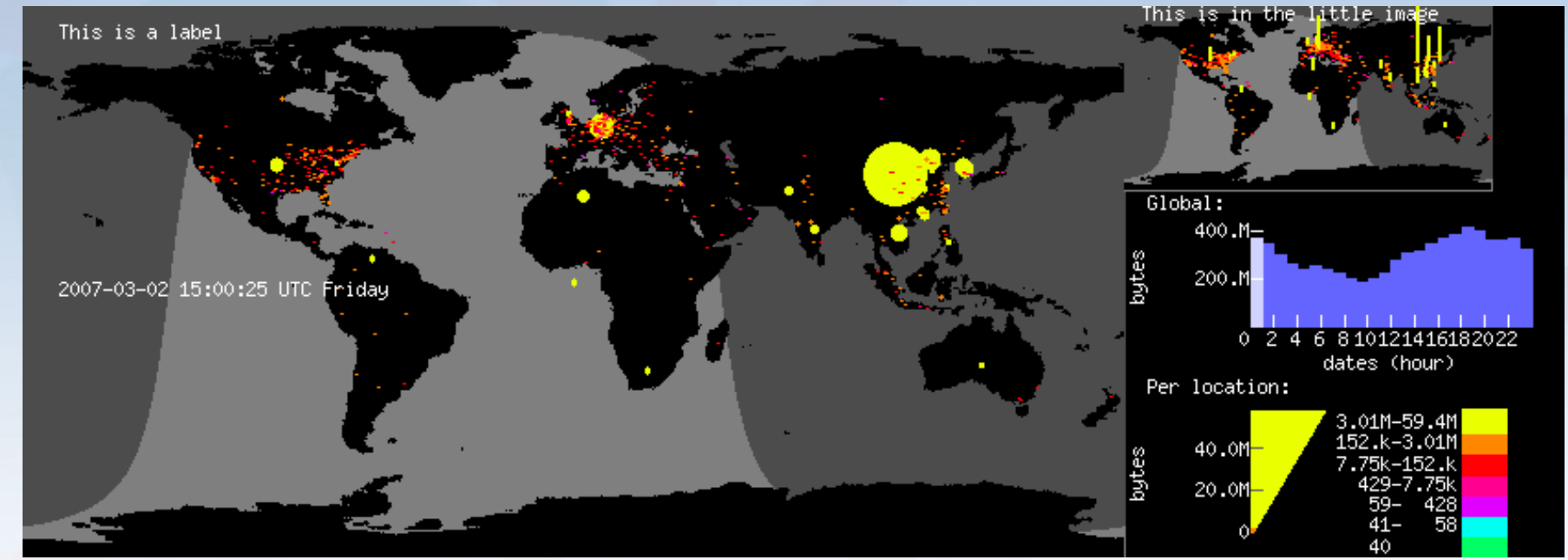
# AusCERT…

AusCERT
Australian Computer Emergency Response Team

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

# Questions?

AusCERT
Australian Computer Emergency Response Team




Graphic representation of DDoS attack against AusCERT in March 2007