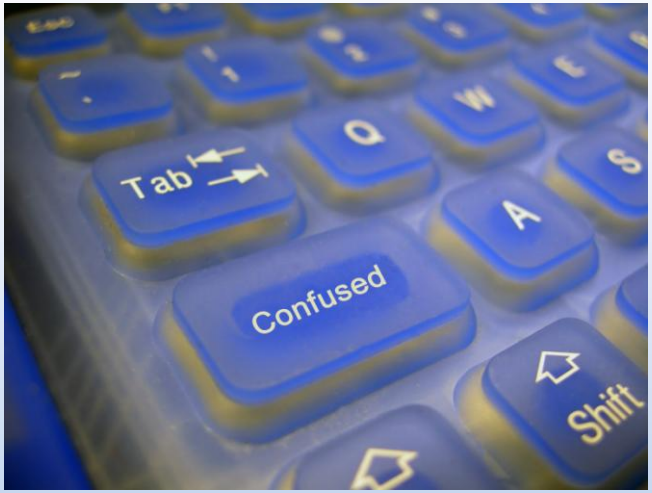
Clouds: In our way or enabling change?

Mike Holm

Operations Manager

QUESTnet, July 2013

Summary

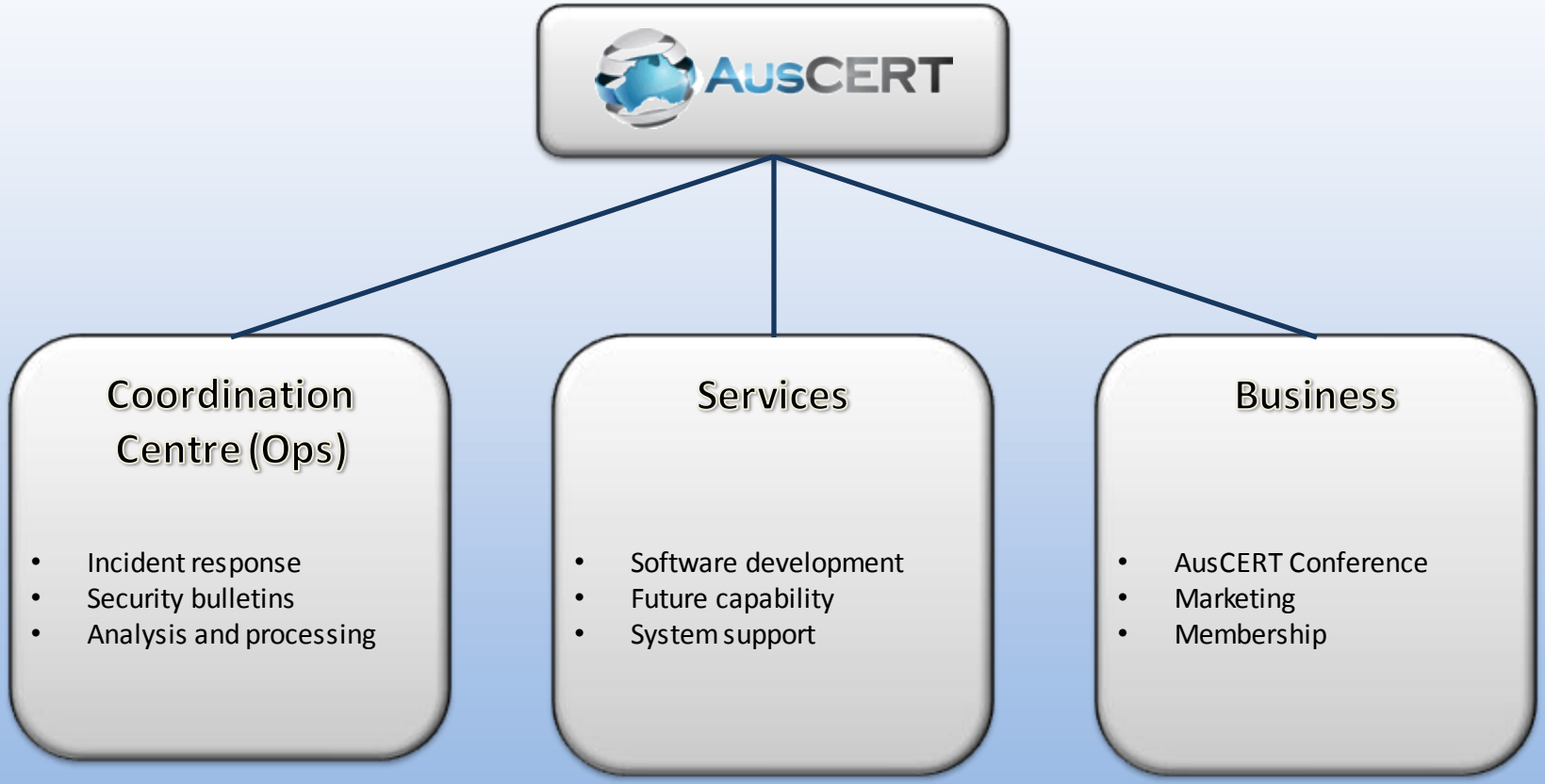


1. Who is AusCERT?
2. Trends: what does AusCERT see coming our way?
3. How do I take control?
4. Carna Botnet: the real story

AusCERT is:

- An **operational** computer emergency response team (CERT) with 20 years experience
- University-based, non-government
- Independent and impartial
- Self-funded and not-for-profit

AusCERT's people



AusCERT's incident response

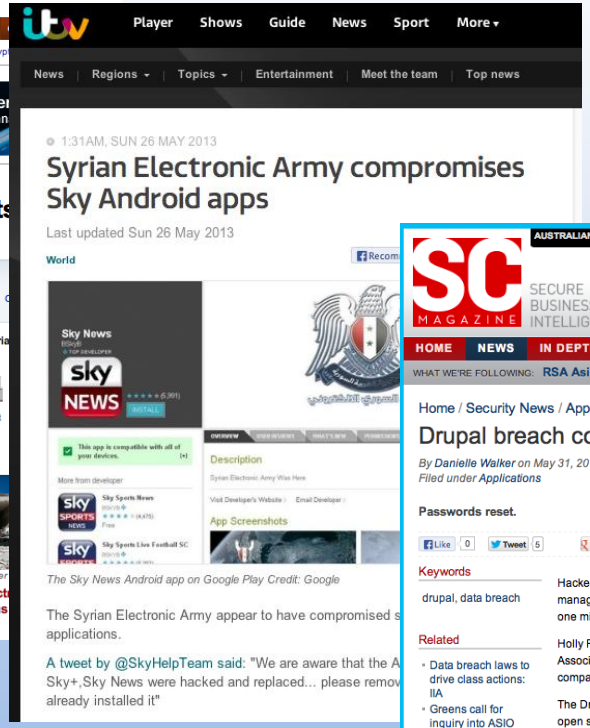
- Notification and repatriation
- Assistance for members

- Compromised web sites
- Botnet CnC, drones
- Publicly disclosed data
- Vulnerabilities in software products
- Malware
- Phishing and other scams

AusCERT's Services

- **Incident response** assistance – proactive and reactive.
- **Security bulletins** via web, email and RSS tailored to each individual's area of interest.
- **SMS Early Warning Alert Service** (unlimited mobile phones).
- **Papers and blogs** providing analysis and trends for information security managers.
- **Malicious URL feed** (blacklist).
- The AusCERT **Remote Monitoring Service** (ARMS).
- AusCERT **Certificate Service** for education and research organisations.
- The highly regarded **AusCERT information security conference**, tutorials and vendors exhibition at substantial discount rates.

In the news: Data breaches



In the news: Ransomware

AusCERT's view of the world

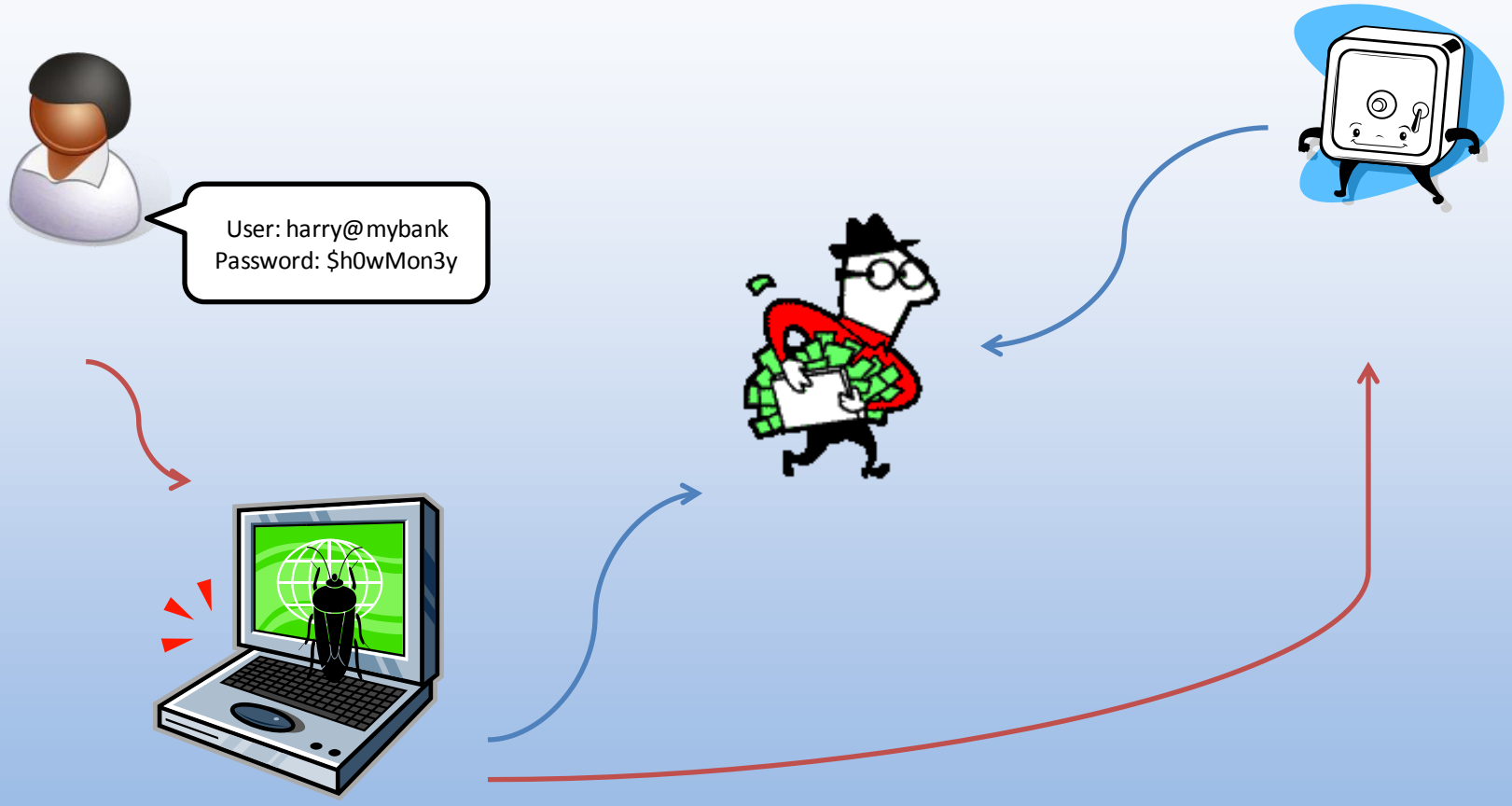
A trip down memory lane…

Phishing & other scams

- Online dating and mule scams – low technology
- Phishing attacks – medium technology
  - Banks, online share trading
  - Email systems
  - Social networking websites
  - eBay, PayPal
- How did the world solve these problems?
  - Well, we didn't really!
  - We tried to educate against scams, with some success.
  - Then the scams got better!
  - **However consumers are largely protected against financial loss by law**

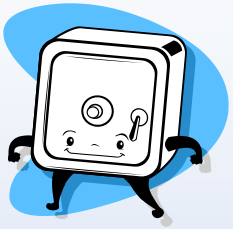
Next, enter the high tech scams

Password loggers!



Even higher tech scams

Bug in the middle!



You type this:

But your bank sees this:

From Account:	To Account/Payee:	Amount $
Savings	Fred	$100

From Account:	To Account/Payee:	Amount $
Savings	Mr Bad Guy	$10,000

Where to next?

Where to next?

- Targeted ransomware
- Targeted attacks using “watering holes”
- Targeted attacks using “spearphishing”
- New types of phishing

New types of phishing

- Universities targeted
- Credentials stolen via phishing
- Used for spam distribution

...Or could it be a reconnaissance for more?

New types of phishing

- The Anti Phishing Working Group noted an increase in 2012 of phishing across multiple domains in shared hosting scenarios.
- Less work for the phishers!

http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf

How can I take control?

- Due diligence of outsourced operations (such as websites).
- Risk assessment (and incident response planning!)
- What do I do if:
  - My brand is phished?
  - My infrastructure is used in a phishing attack?

Watering holes and spearphishing

- Spearphishing: an old but dangerously effective method.
- In 2011, attackers targeted RSA staff with an Excel sheet “2011 Recruitment plan.XLS” which installed a backdoor via a yet-to-be discovered Adobe Flash vulnerability.
- The backdoor connected via the Internet to the attackers allowing control and exfiltration of data.

- https://blogs.rsa.com/anatomy-of-an-attack/

Watering holes and spearphishing

- Watering hole attack: take a trusted website used by a wide group, turn it into an attack vector.
- Apple, Facebook, Microsoft and Twitter employees fell victim via a popular iOS mobile developers' forum.

How can I take control?

- Plan for social engineering attacks.
- User education – does it work?
- Implement controls which segregate critical systems and data.

Ransomware case study

How?

- Access was gained by an insecure remote access system used by the medical practice.

When?

- Over a period of several weeks.
- After initial access was gained, the attacker gathered intelligence and deployed his attack.

What?

- The attacker took control of the medical practice database.
- Two types of regular backup were used by the practice. The attacker disabled one and took control of the other.

The damage?

- The practice database was unavailable.
- A ransom demand was made for $4,000.

How can I take control?

Make sure you oversee your IT provider's operations. Ask:

1. What are the **incident response** and **disaster recovery plans**? What **service levels** apply?
2. Are backups regular, stored in a physically separate location and tested?
3. Are software updates applied in a timely manner?
4. Has the environment been **reviewed against a standard**, eg DSD's Top 35? Has a third party performed a review?
5. Do you have remote access from the Internet? Does it use a secure VPN (virtual private network), or has the insecure "terminal services" port been exposed?
6. Are all computers firewalled and running antivirus software?
7. Have network devices been updated and default passwords changed?
8. What **information security management plan** is in place? Does it adhere to the ISO27000 series for security/risk?

Compromised Devices of the Carna Botnet

(also known as 'Internet Census 2012')

Parth Shukla

Information Security Analyst

AusCERT

pparth@auscert.org.au & twitter.com/pparth

What is the Internet Census 2012?

- /0 port scan of the (allocated) IPv4 ranges
- Results were released Mid-March by an anonymous researcher along with a paper on it.
  - http://internetcensus2012.bitbucket.org/paper.html
- Results contain 9 TB of logs (pure text!)
- Publicly available for download through a torrent as 568 GB of highly compressed (ZPAQ) files

What is in the 9 TB of data?

- ICMP Ping (52 billion records)
- Reverse DNS (10.5 billion records)
- Syncscans (71 billion ports scanned)
- **Service Probes** (175 billion records, 4000 billion requests)
- TCP IP Fingerprint (80 million records)
- IP ID Sequence (75 million records)
- Traceroutes (68 million records)

How is this feasible?

- Maximum of 4,294,967,296 IPv4 Addresses
- Using 1 device and 1 second per IP, it would take:
  4 billion seconds ≈ 126.8 Years
- But with 420,000 devices it would only take 2.6 hours!
- In under 24 hours you can easily collect all the data you need for all allocated IPv4 ranges!
- For problems of logistics and how the researcher handled collection of the data refer to the Internet Census 2012 paper

What is in the Carna Botnet?

- Millions of compromised devices (exact # not published)
- ≈1.2 million of these had “ifconfig” on them so they could be identified
  - 420 Thousand of these were used to perform Internet Census 2012
- 70% of vulnerable devices too small, don’t run linux or somehow limited (e.g. no ifconfig)
  - Traceroutes of **some** of these devices in the public torrent
  - The device must have had the traceroute command for this to happen!

This presentation

- About the ≈1.2 million identifiable compromised devices
  - This data obtained directly from the anonymous researcher
  - Used for analysis for the rest of the presentation
  - NOT publicly available!
- From now on Carna Botnet = 1.2 million identified devices = Compromised Devices of the Carna Botnet
- This botnet unusual because it's not created by phishing, exploiting a coding error or social engineering!

How to be part of the Carna Botnet?

1. A device must be directly reachable from the Internet
2. Telnet running on default port 23 (with no firewall for protection)
3. Allow login using one of the default credentials
   - E.g. admin:admin, admin:password, root:password etc
4. Not just make 1 mistake but 3 mistakes to be part of this botnet!

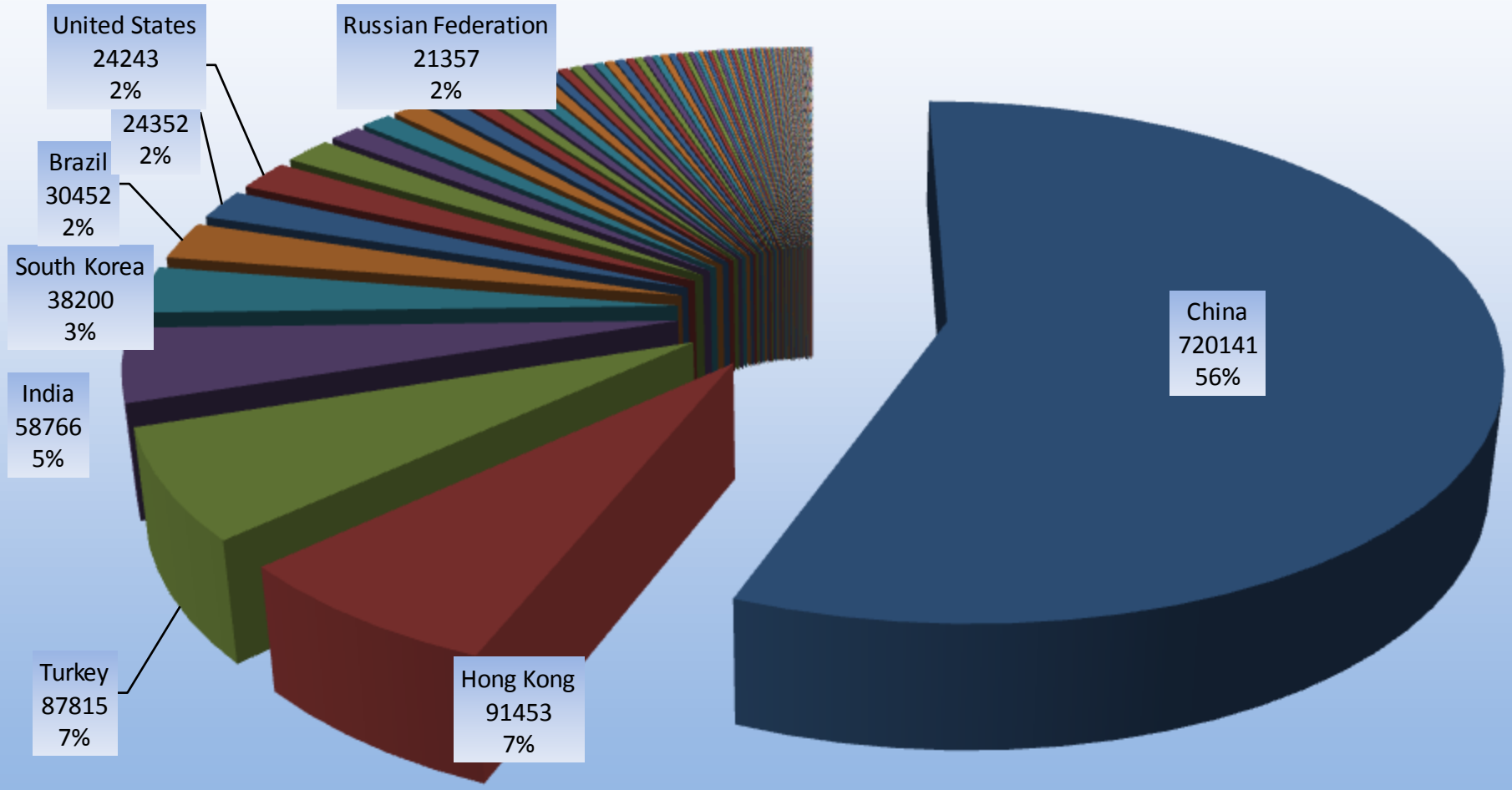
What does the data contain?

1. **MAC address** with the last byte replaced by an ascending number
2. **Manufacturer** - assumed derived from MAC address
3. **RAM** - assumed to be in kilobytes as that's in /proc/meminfo
4. **Uname** - output of uname -a
5. **CPU Info** - output of /proc/cpuinfo
6. **IPs** - list of all IPs associated with this device. Last byte of each IP was zeroed by researcher. Accuracy of each IP to within a **C class**.
7. **Country Code** - two letter country code for each of the IPs. Assumed to be correct at the time the device was compromised.

In the 1,285,192 records there were:

- 200 unique country codes
- 2,058 unique device manufacturers
- 3,881 different RAM sizes
- 10,875 unique unames (system information)
- 35,997 unique CPUs
- 787,665 unique IP Ranges (C class)

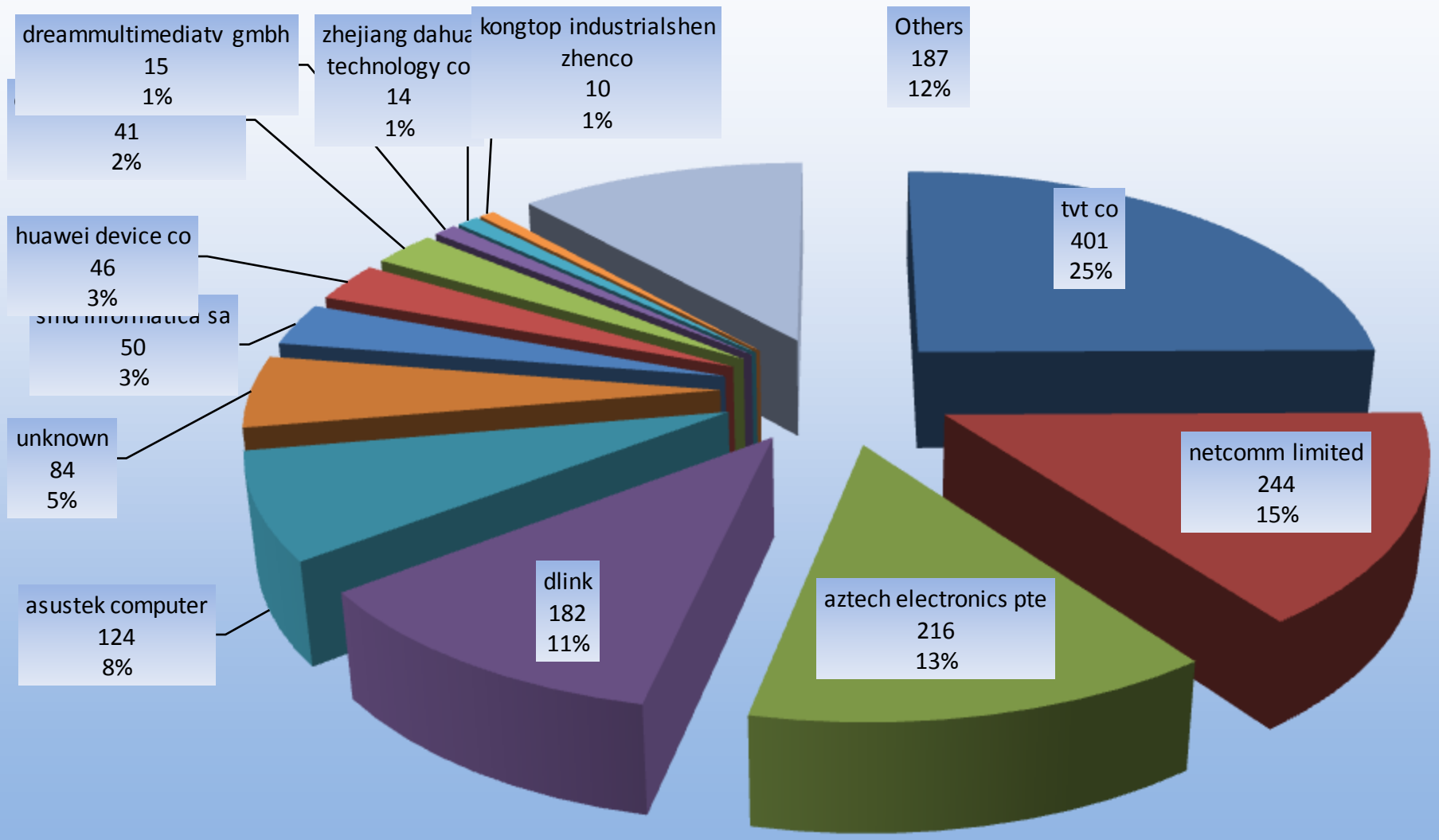
Compromised Devices by Country



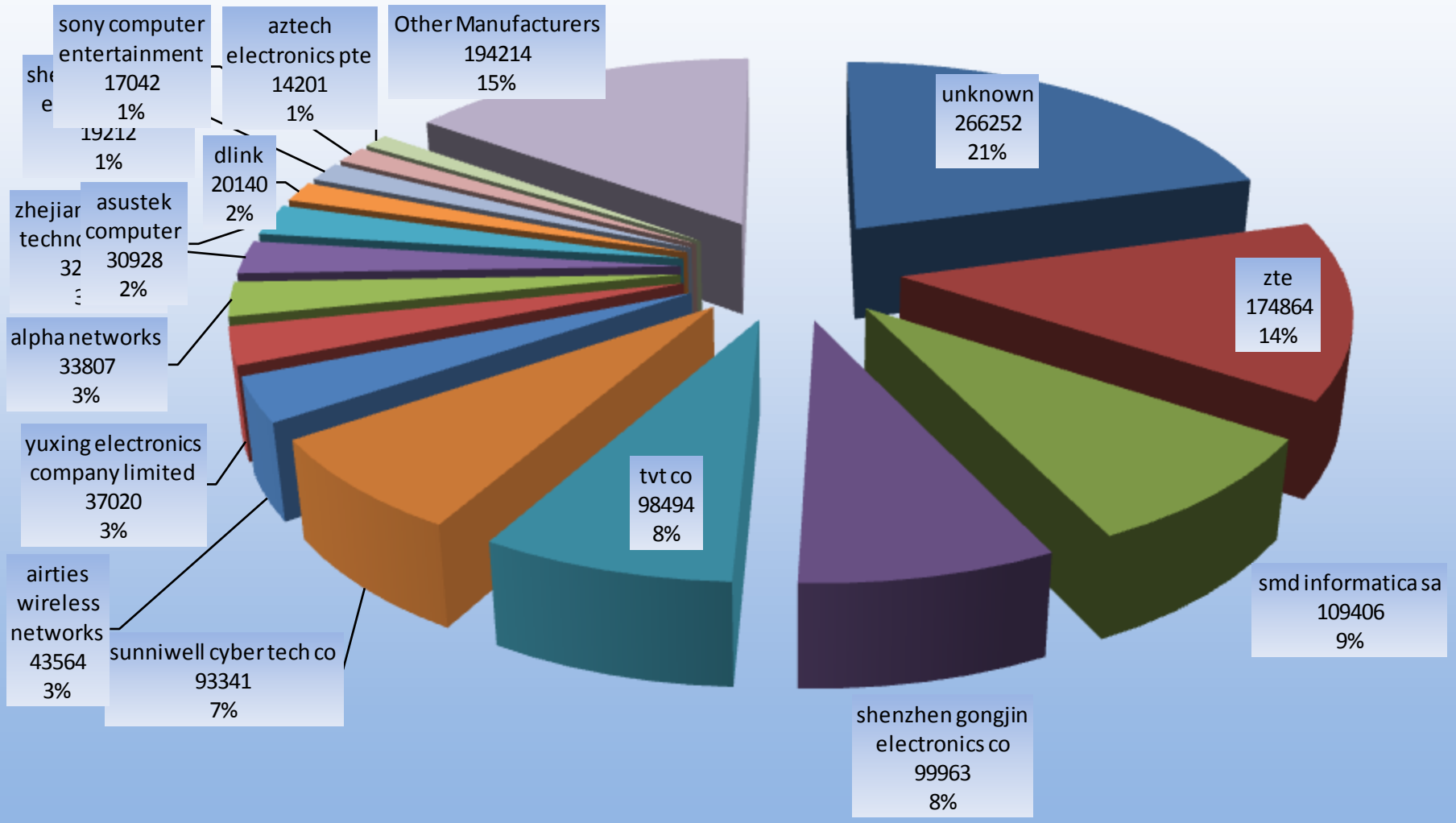
Where is Australia?

- Only 1,614 devices in Australia (0.13% of total records)
  - This is 61% of records for the Oceania region
- Good sign for Australia to have only 0.13% of world compromised devices
- Let's have a quick look at device manufactures of the compromised devices in Australia.

Distribution of Manufacturers in Australia



Worldwide Distribution of Manufactures



So why so many devices?

- Given the prominence of certain manufactures, it seems obvious that most devices in the data are not because of 'stupid' people.
- Certain devices by certain manufacturers may:
  - not allow the change of default logins for telnet.
  - Have a 'backdoor' hardcoded with default credentials perhaps to allow for remote diagnostics. (ISPs could have requested this!)
  - Lack of documentation that there is even a telnet server running on it!
    - what device wouldn't you bother looking for an open telnet port?
  - Require devices to have Internet Reachable IP to benefit from full functionality of the product (i.e. remote viewing of CCTV camera)

What has AusCERT done?

- Relevant data has been supplied to APCERT members and to CERTs from any country with more than 10 thousand compromised devices.
  - Adds up to about 22 countries in total.
- Working on best strategy to tackle this problem for Australia
  - Without timestamps, most telcos using DHCP can't do anything!
- Working with IEEE to obtain official contact list for manufacturers
  - So we can work with manufacturers to bring awareness to them and pubic.
- This presentation!
  - Publication of what has been covered in this presentation and more to come
- Please spread the word – public awareness is vital.

How can I take control?

Resources:

1. **DSD Strategies to Mitigate Targeted Cyber Intrusions**

   https://www.auscert.org.au/16633

2. **Ransomware, today and tomorrow**

   https://www.auscert.org.au/17155

3. **Carna Botnet**

   http://bit.ly/auscertcarna

Thank you!

Questions?

auscert@auscert.org.au

https://www.auscert.org.au/

https://www.facebook.com/AusCERT/

https://twitter.com/auscert