



Clouds: In our way or enabling change?

Mike Holm

Operations Manager

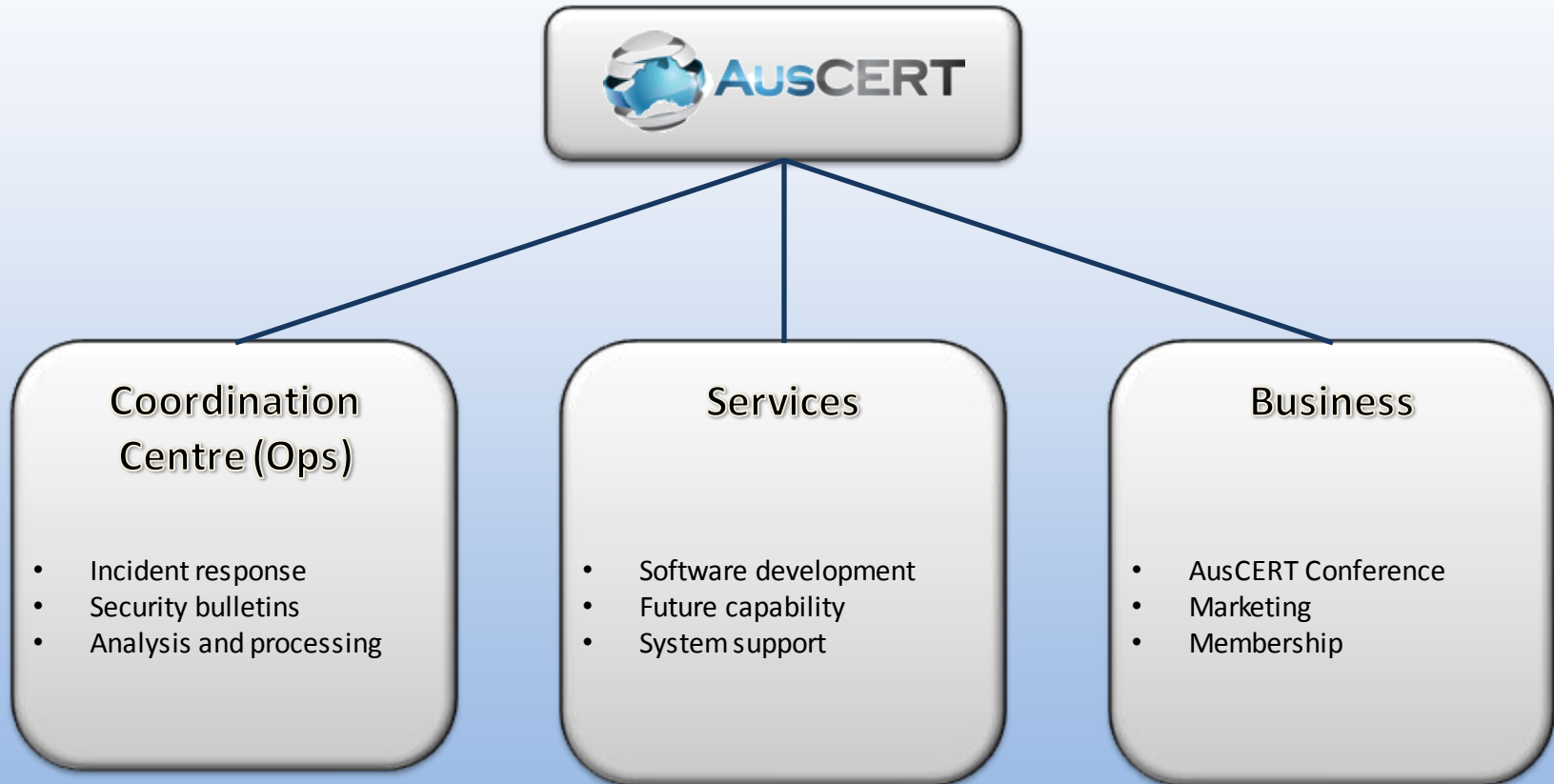
QUESTnet, July 2013

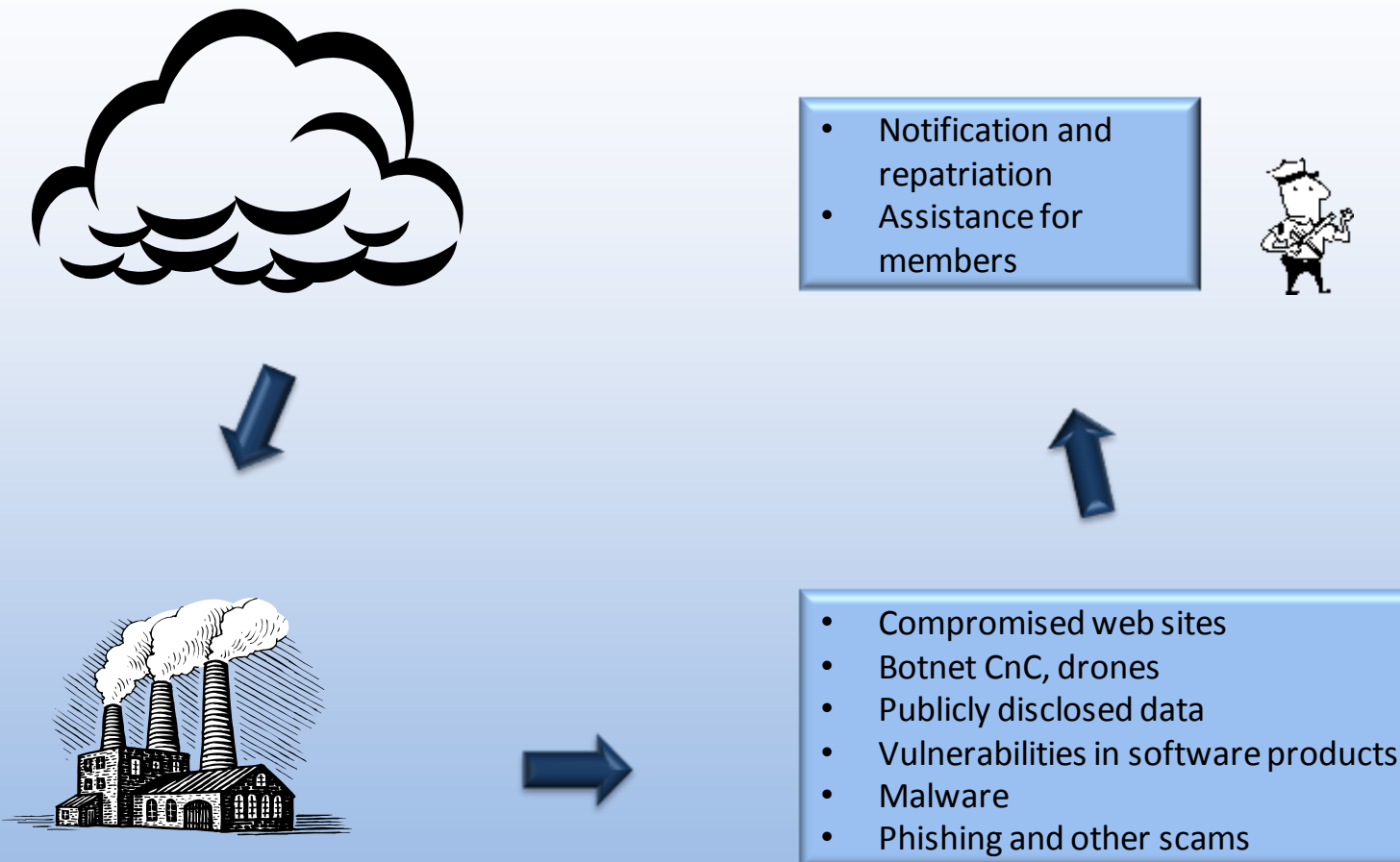


1. Who is AusCERT?
2. Trends: what does AusCERT see coming our way?
3. How do I take control?
4. Carina Botnet: the real story



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





- **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



ZDNet

Hot Topics | Newsletters | Reviews | Downloads | White Papers

Asia Edition | Next-Gen Networks | TechBiz | Security | India | CXO | Telcos | Startups | Singapore

MUST READ: [Microsoft unleashes bug bounty program](#)

Topic: Security | Discover | Follow via: RSS

Hackers breached Washington state court with Adobe ColdFusion flaw

Summary: Hackers used Adobe software to stage a data breach that left up to 160,000 Social Security numbers exposed.

By Liam Tung | May 10, 2013 -- 11:10 GMT (19:10 SGT)

Follow @liamtung

Hackers used a flaw in Adobe's ColdFusion software to breach Washington state's Administrative Office of the Courts.

The hackers may have accessed as many as 160,000 Social Security numbers and up to one million drivers license numbers, according to a statement by the court on Thursday.

The court has only confirmed that 94 Social Security numbers were definitely taken, however, it believes the breach occurred sometime between last autumn and February this year, according to Associated Press. It also confirmed the breach happened due to a flaw in Adobe's web application platform, ColdFusion.



InformationWeek Security

Software | Security | Cloud | Mobility | Social Business | Big Data | Windows | Global CIO

Attacks/Breaches | Application Security | Vulnerabilities | End User/Client Security | Encryption

Powered by Cisco | Unlimited Potential | Cisco Power Cloud and Managed Start Here >

Yahoo Japan Data Breach: 22M Accounts Exposed

NEWS

Mathew J. Schwartz

See more from Mathew

Connect directly with Mathew: Bio | Contact

Start the Discussion

33 | 81 | 3 | 19 | 0

Like | Tweet | +1 | Share | Submit

Mail | Print

Mathew J. Schwartz | May 20, 2013 12:31 PM

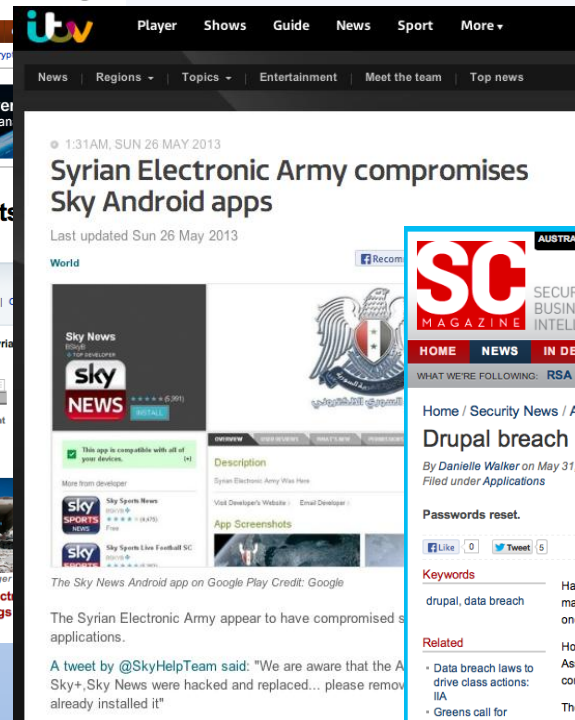
Yahoo disclosed Friday that a breach at Yahoo Japan may have exposed 22 million login names to attackers.

"We don't know if the file [containing 22 million user IDs] was leaked or not, but we can't deny the possibility, given the volume of traffic between our server and external terminals," read a statement issued Friday by Yahoo Japan. Yahoo is the country's most-visited website, and is jointly owned by Yahoo and Japanese network operator Softbank.

Yahoo Japan posted a link to a related breach notification on its website.

MORE SECURITY INSIGHTS

The Syrian Electronic Army: 9 Things You Know



iTV | Player | Shows | Guide | News | Sport | More >

News | Regions | Topics | Entertainment | Meet the team | Top news

1:31AM, SUN 26 MAY 2013

Syrian Electronic Army compromises Sky Android apps

Last updated Sun 26 May 2013

World

Sky News

This app is compatible with all of your devices.

More from developer

Sky Sports News

Sky Sports Live Football SC

The Syrian Electronic Army appear to have compromised Sky News Android apps.

A tweet by @SkyHelpTeam said: "We are aware that the Sky+ Sky News were hacked and replaced... please remove already installed it"



SC MAGAZINE | AUSTRALIAN EDITION

SECURE BUSINESS INTELLIGENCE

POPULAR: authority, certificate, certification

HOME | NEWS | IN DEPTH | REVIEWS | EVENTS | RESOURCES | SC AWARDS

WHAT WERE FOLLOWING: RSA Asia Pac | Carding and fraud | Jobs | Print edition

Home / Security News / Applications

Drupal breach compromised a million accounts

By Danielle Walker on May 31, 2013 3:34 PM

Filed under Applications

Passwords reset.

Keywords

Drupal, data breach

Related

- Data breach laws to drive class actions: IIA
- Greens call for inquiry into ASIO blueprint theft
- ITV and Sky hacked by the Syrian Electronic Army
- Data breach notification law introduced to Parliament
- ASIO blueprints,

Hackers ransacked the servers of Drupal.org, an open source content management platform, to plunder the sensitive information of nearly one million accounts.

Holly Ross, executive director of the Portland, Ore.-based Drupal Association, said a vulnerability in third-party software installed on company servers enabled the intrusion.

The Drupal Association is the nonprofit organization that supports the open source CMS project Drupal, which is not a commercial entity. Drupal software is offered free for download, and is comparable to other popular content management systems like WordPress.

In a Wednesday blog post, Ross said usernames, email addresses, country information, and hashed passwords were exposed in the incident. All passwords were hashed, while only some were salted, an additional security layer where a sequence of symbols is added to passwords before they're hashed.

Most Recent

- Scores of uncovered
- Drop box within
- Inside the
- Hacking 1
- Back Trac

LATEST

- Klaus 11
- on Windo
- for Hyper
- McAfee 1
- days ago

Davefe

against th

In the news: Ransomware



AFP
AUSTRALIAN FEDERAL POLICE

All activity of this computer has been recorded
If you use a webcam, videos and pictures were saved for identification



Video recording: ON

You can be clearly identified by resolving your IP address and the associated hostname

Your IP Address: [redacted]
Your Hostname: [redacted]
Location: Australia

Your Computer has been locked!

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 27A - Copyright
A fine or imprisonment for the term of up to 4 years (the use or sharing of copyrighted files - movies, software)

Article 193 - Pornography
A fine or imprisonment for the term of up to 2 years (the use or distribution of pornographic files)

Article 188 - Pornography involving children (under 18 years)
Imprisonment for the term of up to 15 years (the use or distribution of pornographic files)

Article 104 - Promoting Terrorism
Imprisonment for the term of up to 25 years (you have visited websites of terrorist organizations)

Article 105 - Misleading computer use - installing malware

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of 100 AUD.

1. 
2. 
3. 
4. 



You can get Ukash from hundreds of thousands of global locations, online, from wallets, from Visa and ATMs

Exchange your cash for a Ukash voucher and use your voucher code in form below.

Code:

1 2 3 4 5 6 7 8 9 0

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.

Where can I buy Ukash?

[Prepaid4.me](#)

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.





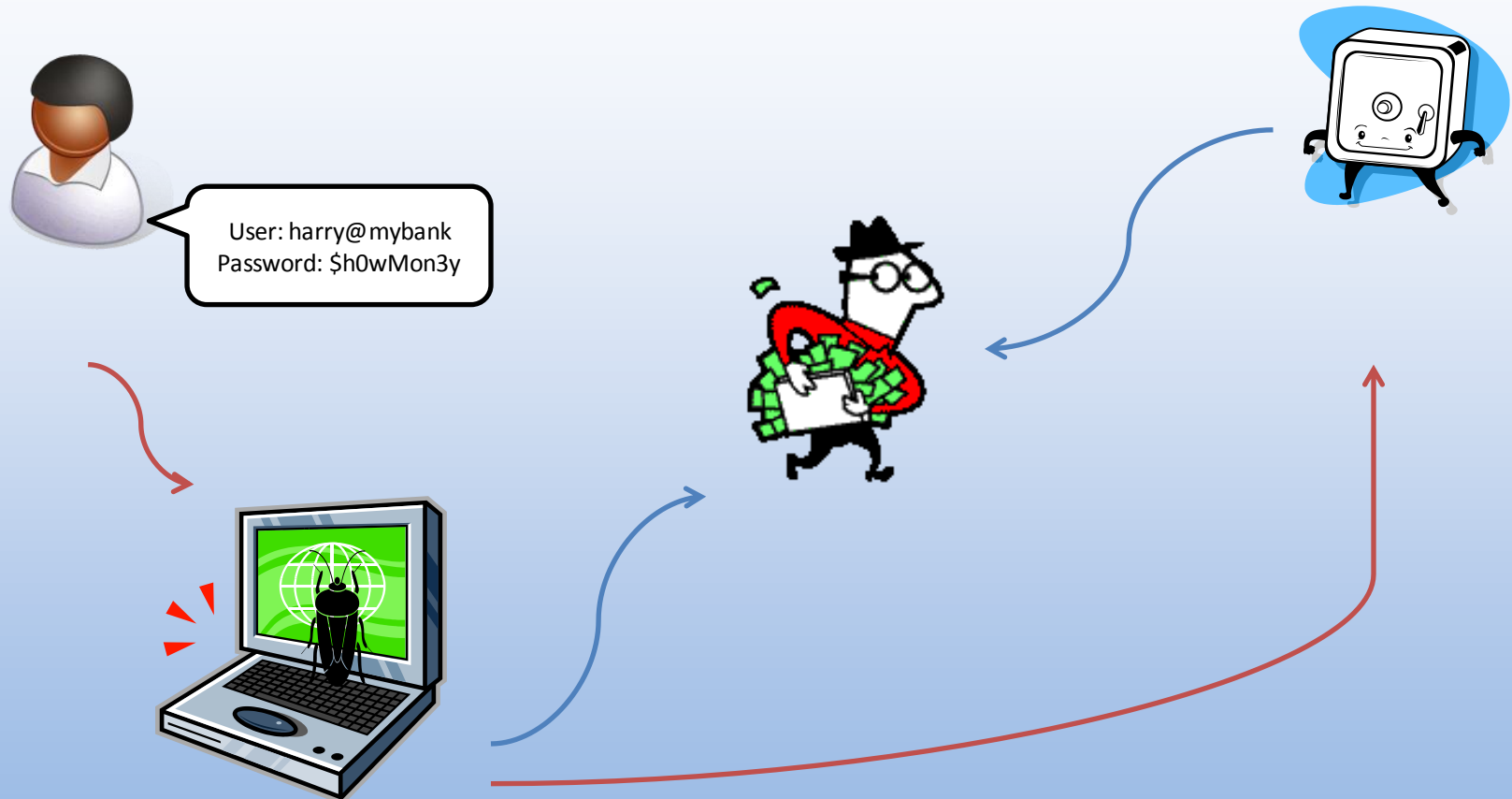


A trip down
memory
lane...

- 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**

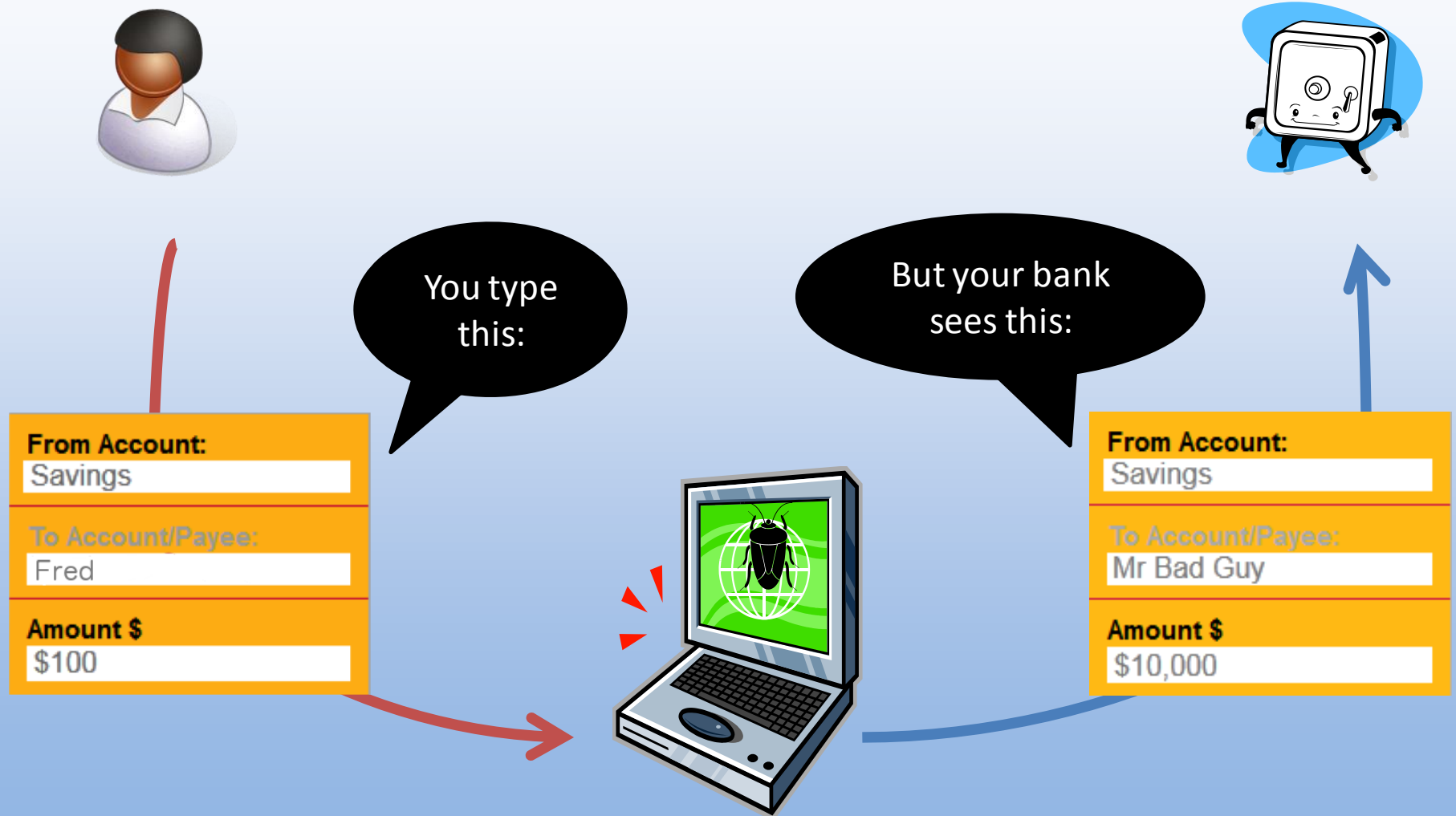
Next, enter the high tech scams

Password loggers!



Even higher tech scams

Bug in the middle!



Where to next?

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

- Universities targeted
 - Credentials stolen via phishing
 - Used for spam distribution
- ...Or could it be a reconnaissance for more?

- 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



- 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?

- 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 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.

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.

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 $\approx$ 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!

- 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!

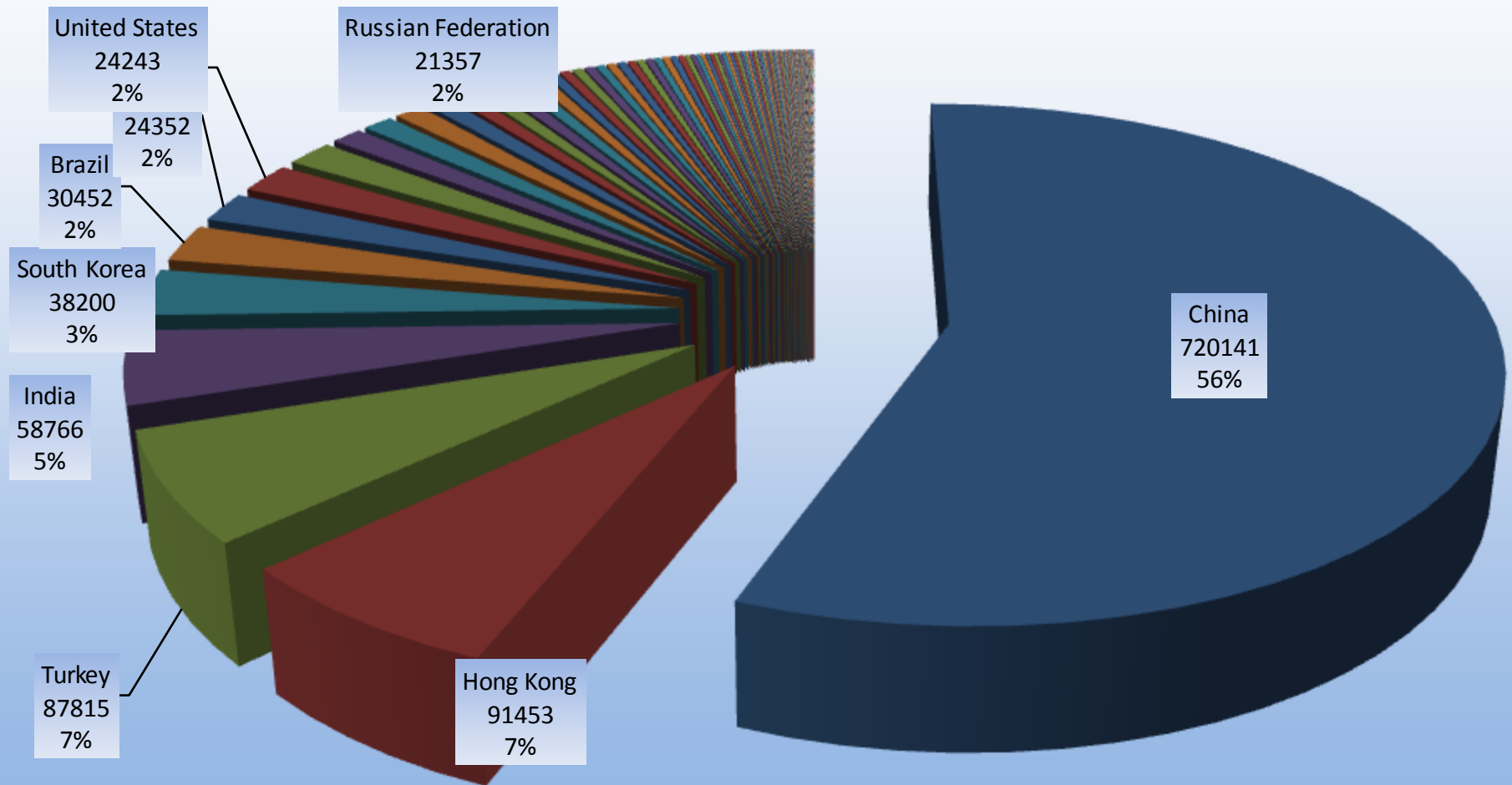
What does the data contain?

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:

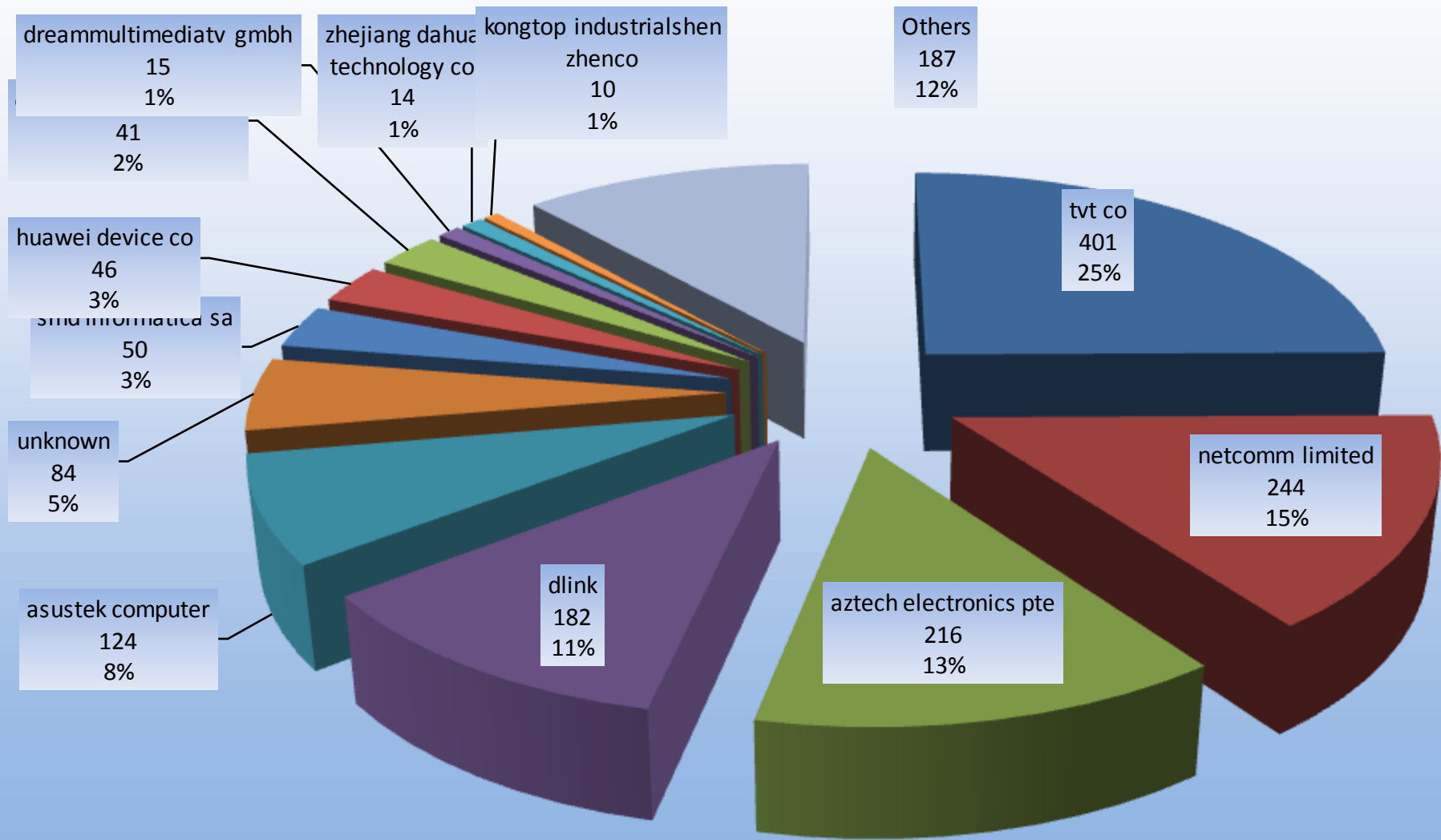
- 200 unique country codes
- 2,058 unique device manufacturers
- 3,881 different RAM sizes
- 10,875 unique unames (system information)
- 35,997 unique CPUs
- 787,665 unique IP Ranges (C class)

Compromised Devices by Country

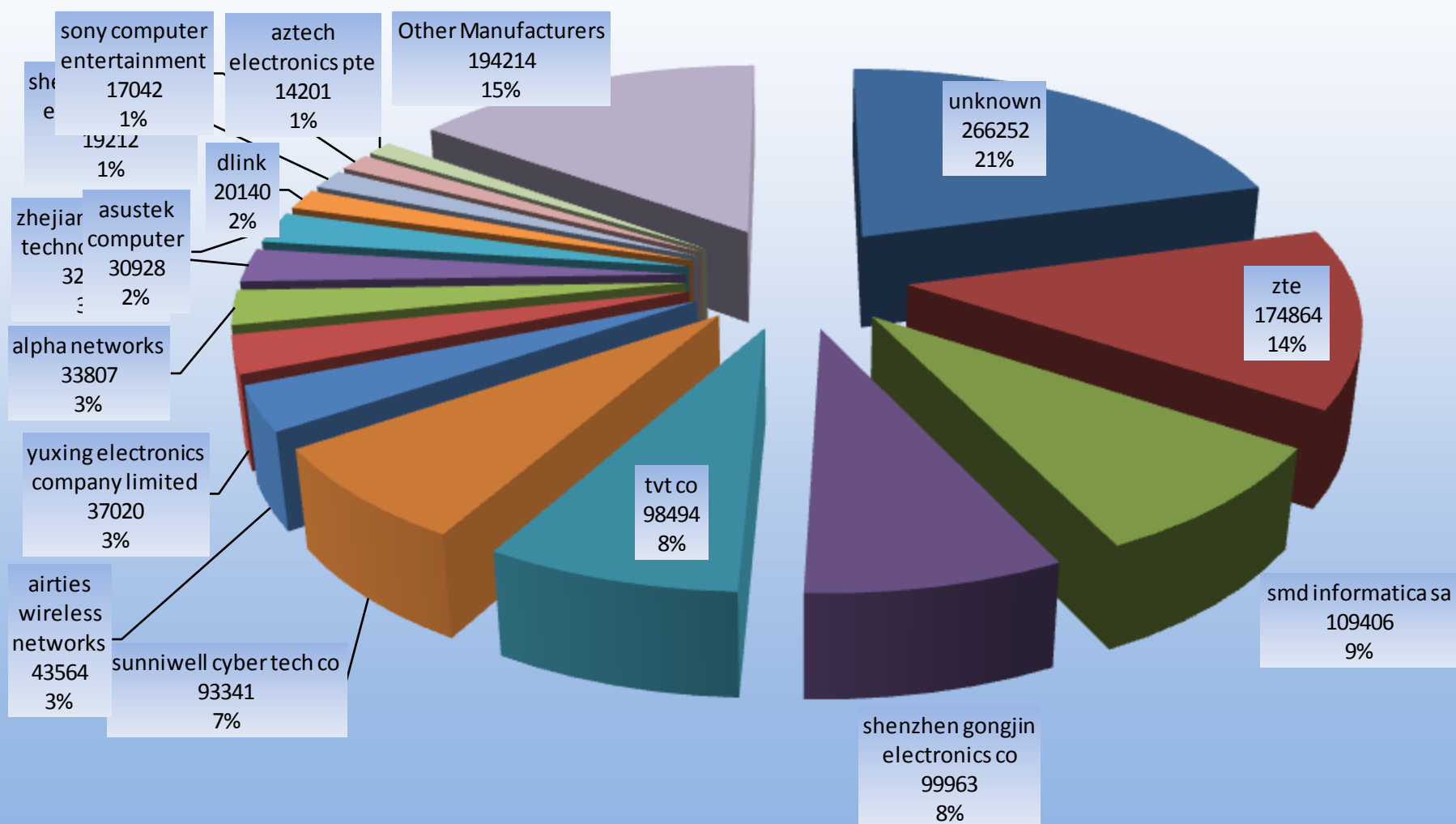


- Only 1,614 devices in Australia (0.13% of total records)
 - This is 61% of records for the Oceania region
- Good sign for Australia to have only 0.13% of world compromised devices
- Let's have a quick look at device manufactures of the compromised devices in Australia.

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)

- 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 public.
- This presentation!
 - Publication of what has been covered in this presentation and more to come
- Please spread the word – public awareness is vital.

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>