AusCERT
Australian Cyber Emergency Response Team

QUESTnet

QUESTnet 2016
AusCERT Update

Mike Holm, Operations Manager, AusCERT

mike@auscert.org.au | 0417 440 189

Agenda

- What is AusCERT
- Maximising the value of AusCERT services
- SOC (Security Operations Centre) and ISAC (Information Sharing and Analysis Centre) models for Higher Education
- CAUDIT survey on AusCERT ISAC model
- Our own ideas for the future
- Group discussion

Takeaways (slides available for download later)

- AusCERT's Incident Handling infographic
- How to set up and maximise AusCERT services

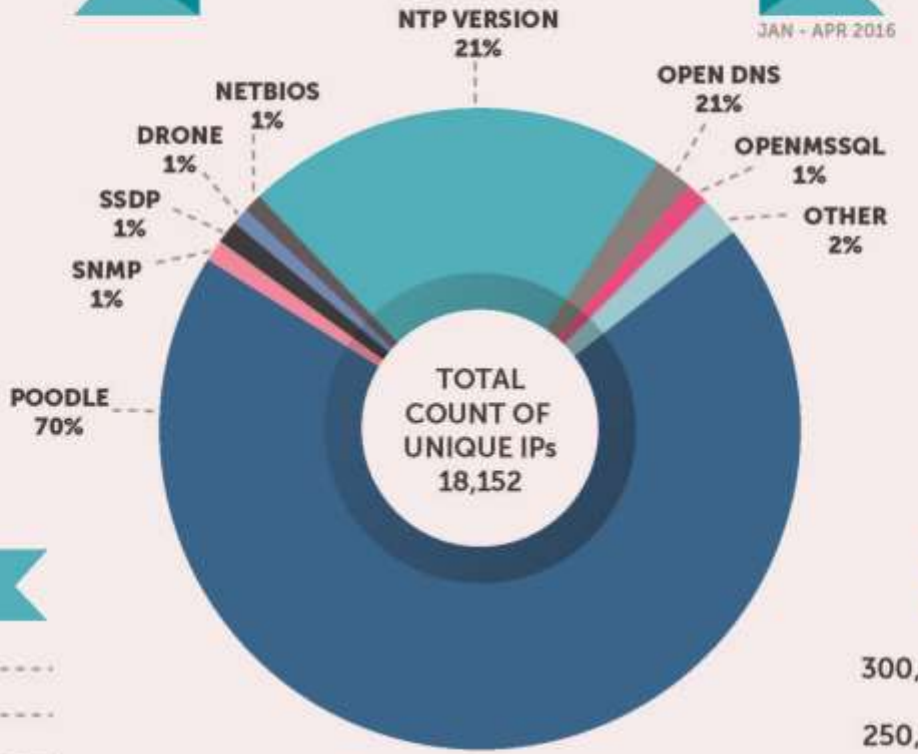
WHAT AUSCERT IS SEEING & DOING

10 MAY 2016

NUMBER OF UNIQUE MALWARE SAMPLES AUSCERT SENDS TO AV VENDORS ON AVERAGE EACH MONTH

MSINs UNIQUE IPs

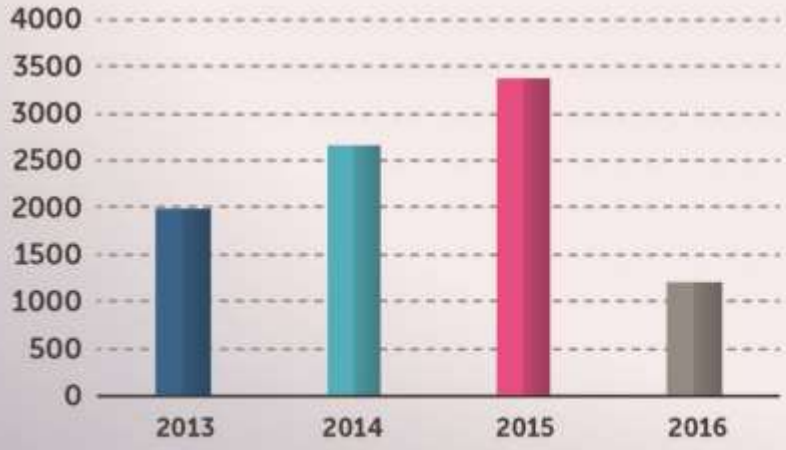
JAN - APR 2016



THE PERCENTAGE OF SAMPLES THAT ARE DETECTED BY AV VENDORS WHEN MALWARE IS SUBMITTED BY AUSCERT (ACROSS 59 VENDORS)

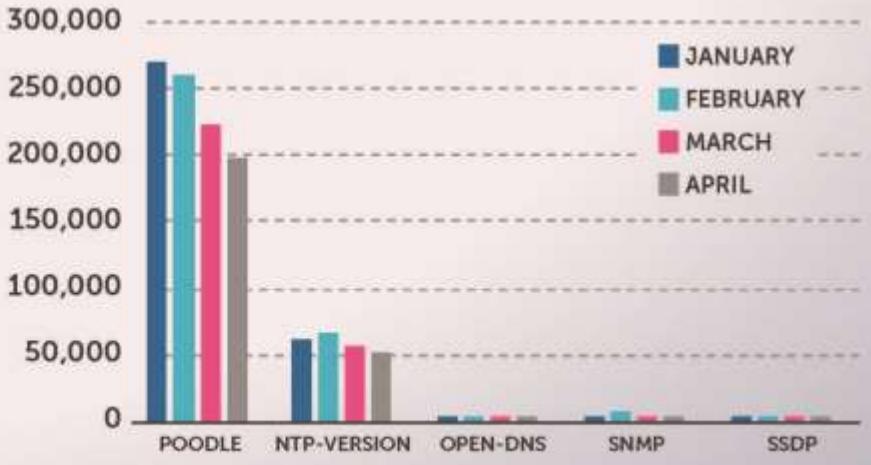
AUSCERT SECURITY BULLETINS

10 MAY 2016



AVERAGE NUMBER OF PHISHING AND MALWARE SITES AUSCERT PROCESSES EACH MONTH

MSINs TOP VUNERABLE HOSTS BY MONTH



AusCERT Membership Services

- Security bulletins via email, web, profile email, RSS
- SMS early warning service
- Members IRC channel
- Proactive and reactive incident management services
- 24/7 member hotline for incident response assistance
- Flying Squad and VISO services (additional fees apply)
- Malicious URL feed
- AusCERT Remote Monitoring Service (ARMS)
- Phishing takedown service
- Certificate Service

Security Bulletin Service

Set up mailing list – Security Bulletins

- Goal: Set up your internal distribution lists to receive security bulletins
- Security bulletins
  - auscert-member@yourdomain.edu.au (or equivalent)
  - Allows you to add any number of internal users to receive ALL bulletins
  - You manage who is added and removed from the list within your organisation
  - Volume can be managed by creating rules within your email client
  - If you subscribe to profile email, you will receive duplicates

Reference: Security Bulletins https://www.auscert.org.au/1

Proactive Incident Response

Set up access to member only portal

- https://www.auscert.org.au/login.html
- AusCERT creates a primary web account (for the Primary Contact), who can
  - Add or remove internal users to give access
  - Change passwords for these users
- Access to member only portal is needed for:
  - Read ASBs and other member only content
  - Set up profile email
  - Access malicious URL feed
  - Access symmetric keys to decrypt encrypted files sent to by email from AusCERT
  - Get the IRC channel shared password
  - Get the Incident Hotline number
  - Organisation's primary contact grants access (ask AusCERT if primary is unknown)

Reference: Member Portal https://www.auscert.org.au/main/member

Proactive Incident Response

Set up mailing list – incident notifications

- Goal:
  - Set up your internal distribution lists to proactive incident notifications
- AusCERT Contact
  - auscert-contact@yourdomain.edu.au (or equivalent)
  - Allows you to add any number of internal users to receive ALL incident notifications affecting your domains and IPs
  - You manage who is added and removed from the list within your organisation
  - Everyone on this list will see all information affecting your organisation
  - This list will also receive Weekly Incident Summary Reports

Proactive Incident Response

Notifications from AusCERT

- Goal: Ensure correct and prompt action can be taken when AusCERT proactively detects incidents specific to the Member
- Workshop to discuss:
  - Incident response plan
  - MSIN example walkthrough
  - Data leakage notification walkthrough

Reference: MSINs https://www.auscert.org.au/resources/blog/member-security-incident-notifications-msin-launched

=======HEADING FOR INCIDENT TYPE 1========

Incident Type
Name of the incident and any known exploited vulnerabilities and associated CVEs.

Incident Description
Further information on potential attack vectors and impacts.

Incidents Reported
List of individual reports sighted by AusCERT
Incident report 1
Incident report 2
…Incident report n

AusCERT recommended mitigations
Steps for resolution of incidents or mitigation of vulnerabilities which could be exploited in the future.

References
Links to resources referenced within the report

Additional Resources
Links to additional material such as tutorials, guides and whitepapers relevant to the report aimed at enhancing the recipients understanding of the addressed vulnerabilities, potential impacts and mitigation techniques.

==========END OF REPORT==========

Compromised host example:

Timestamp:	2015-08-25T00:20:34+00:00
Drone IP:	123.456.789.abc
Drone Port:	13164
Drone Hostname:	abc.xxx.xxx.xxx.au
Command and Control IP:	aaa.bbb.ccc.ddd
Command and Control Hostname:	xxxxxxxx.yyy.org
Command and Control Port:	80
Malware Type:	redyms

==========

Open DNS resolver example:

Timestamp:	2015-09-27T01:56:10+00:00
IP:	123.45.678.90
Port:	53
Hostname:	abc.def.net.au
DNS Amplification factor:	1.3810
Protocol:	udp

==========
All timestamps are in UTC

Threat data feeds

- Goal: Determine the best use case(s) and assist the Member to utilise AusCERT's threat data feeds
- Workshop to discuss:
  - Existing capability – SEIM, centralised logging, content filtering
  - The value of AusCERT's Malicious URL Feed
  - Possible use cases for the Malicious URL Feed
  - Future of threat intelligence, and how AusCERT can assist the Member from an information security community point of view

Reference: Malicious URL Feed [*https://www.auscert.org.au/9123*](https://www.auscert.org.au/9123)

Reactive Incident Response

How and when to contact us

Operations: For incidents and cyber security advice or questions

- AusCERT 24x7 incident hotline https://www.auscert.org.au/5141
- Email and IRC is monitored during business hours only
- auscert@auscert.org.au
- IRC https://www.auscert.org.au/22670

Membership: General support to access services, ARMs or Member portal

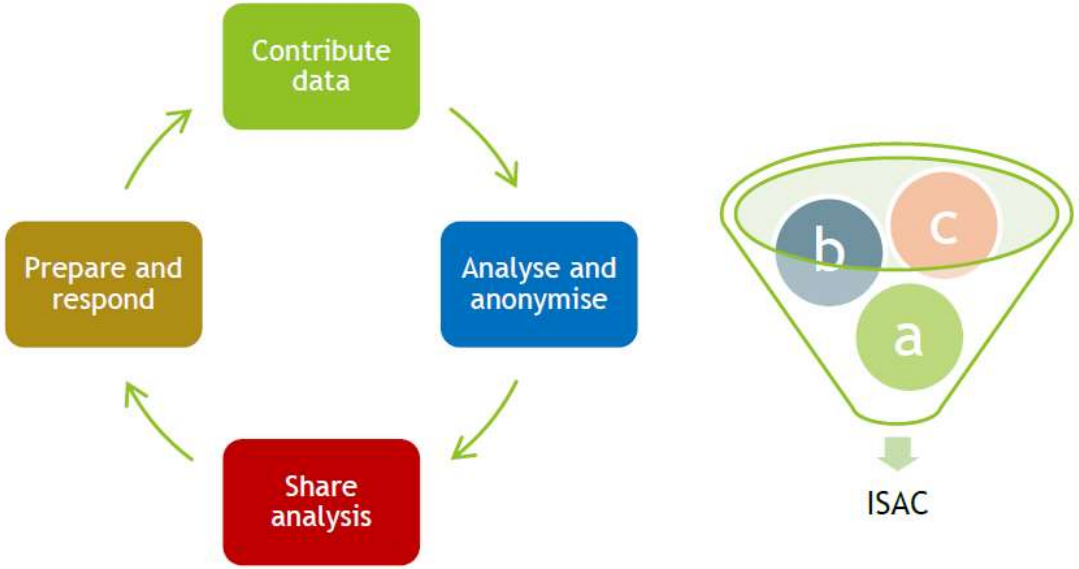
- update your account details (contacts, IP addresses, domains)
- membership@auscert.org.au
- 07 3365 4417

Flying Squad Service

- Purpose
  - For complex and serious cyber security incidents, having on-site support from a trusted information security analyst will be important to help manage the incident. https://www.auscert.org.au/resources/downloads/flying-squad-service-description_3june2016.pdf
- 2 service levels:
  - Best Effort (no guaranteed availability but no fee unless we are available to provide the service)
  - Retainer (guaranteed 24 hour depart to your site with Retainer Fee $24,000 pa
    - Includes up to 5 x 8 hour (business days incident response)
    - If outside of business hours (additional fees payable)
- To be prepared complete the Flying Squad Service schedule before you need to call us
  - https://www.auscert.org.au/resources/downloads/flying-squad-service-schedule-form_3june2016.pdf
  - Best effort – no risk – no cost up front

New for Higher Education Sector

- SOC and/or ISAC services
- Membership driven, transparent, economies of scale for Higher Ed
- AusCERT already has expertise in this area



CAUDIT Survey

- Short Survey on AusCERT ISAC-SOC Proposal

CAUDIT Survey

3. Are you aware of AusCERT's ISAC-SOC proposal?

Yes	12
Not Sure - I'd like more	1
No	0

6. At what level in your institution is there awareness of the ISAC proposal?

Director or Associate Di	9
Cybersecurity Manager	2
Executive Level	2

4. Is your institution likely to join the ISAC-SOC ? (annual fee estimates vary depending on institution between $2.5k-$33k, refer to the ISAC proposal schedule)

Details

Yes	11
Unsure	2
No	0

8. Would your institution participate in the working party which will define the services to be offered and report back to the CAUDIT Spring Members meeting (if yes please advise contact details for who this will be)?

Details

Yes	12
No	1

Our own ideas

- Your feedback so far asked AusCERT for:
  - Repository of documents, checklists, best practice guides
  - Information sharing on indicators of compromise

- https://www.auscert.org.au/resources/blog/useful-security-resources
- Choosing a managed security service provider (Members only) https://auscert.org.au/download.html?f=2058

- MISP (Malware Information Sharing Platform)
  - http://www.misp-project.org/

Navigating Incident Handling with AusCERT Services

❶ PREPARATION

Identify your digital assets:
- Asset inventory
- Network diagrams

Understand your cyber risks
- Conduct a cyber security review and risk assessment*

Develop an Incident Response Plan (IRP)*
- **Use the AusCERT IRP template**

Understand your obligations with regard to breach of PII and breach notification

Communicate and test your IRP*

Ensure you have access to secure back-ups that cannot be corrupted

Have access to secure baseline images for workstations and servers

Ensure you have widespread logging and/or SIEM functionality
- Where outsourced arrangements are in place ensure procedures are established for log data to be sent to you in a timely fashion

Sign up for the Flying Squad Service - 2 service levels
- **Best Effort**
- **Retainer**

Send your PGP key to AusCERT and know where to get AusCERT's current PGP key

Put the AusCERT Incident Hotline number in your IRP

AusCERT VISO can help with*

❷ IDENTIFICATION AND ANALYSIS

Detect incidents
- SIEM alerts
- **Member Security Incident Notifications (MSINs)**
- **ARMS notifications**

Follow your IRP
- Report details of incident
- Establish IR team with clear lines of responsibility and resources
- Report to ACORN
- Record details of actions taken and sequence
- Take images of affected systems for further future analysis

Analyse the incident and identify all affected systems and data

Identify root cause of incidents
- Analyse SIEM log files
- Scan for vulnerabilities in affected and connected systems

- **Review AusCERT security bulletins and the malicious URL feed to identify potentially exploited vulnerabilities**

Assess the impact of the incident
- Refer to the asset inventory and risk assessment
- If PII consult with legal and/or information Commissioner regarding obligations

Contact AusCERT via email, IRC or 24/7 hotline for advice

Seek external support early if potential for serious harm and complex incident

❸ CONTAINMENT

Develop a containment and eradication strategy
- Refer to network diagrams and asset inventories to assist
- Where appropriate disconnect and/or isolate affected systems from the network and/or through use of ACL
- Change passwords

For phishing incidents
- **Contact AusCERT to request site take down**

For malware incidents
- **Submit malware sample to AusCERT to send to AV vendors**

Contact AusCERT via email IRC or 24/7 hotline for advice

Seek external support early if potential for serious harm and complex incident

For serious incidents, contact AusCERT and request Flying Squad assistance (2 services levels)

Monitor **MSINs** and SIEM for evidence of ongoing malicious activity

Ensure appropriate attention is given to communications and public relations

❹ ERADICATION

Implement the eradication strategy

Re-install affected systems from trusted baseline images and back-ups

Check that identified vulnerabilities which contributed to the incident have been removed

Monitor **MSINs** and SIEM for evidence of ongoing malicious activity

Contact AusCERT via email, IRC or 24/7 hotline for advice

Seek external support early if potential for serious harm and complex incident

For serious incidents, contact AusCERT and request Flying Squad assistance (2 services levels)

❺ RECOVERY

Reconnect cleaned and re-imaged systems to the network

Advise management and stakeholders that the incident is resolved

Monitor **MSINs** and SIEM for evidence of ongoing malicious activity

Contact AusCERT via email, IRC or 24/7 hotline for advice

❻ LESSONS LEARNT

Conduct a post incident review and identify controls that were assessed to be inadequate that:**
- Contributed to the incident (prevent)
- Hindered the timeliness of detecting the incident (detect), or
- Hindered the efficient and full recovery from the incident (respond)

Write up post-incident report**
- identify cause and impact of the incident
- actions taken

Review adequacy of IRP and internal policies and procedures relating to the handling of the incident**

AusCERT VISO can help with**

Make recommendations regarding adequacy of existing security controls, policies and procedures relating to prevent, detect and response capabilities

Report to management and seek authority to address changes to avoid similar issues in future

AusCERT's PGP Key is available here: https://www.auscert.org.au/1967
Log into https://www.auscert.org.au/5141 to get the member only AusCERT Incident Hotline number
Membership enquiries: **1800 648 458**

AusCERT

VERSION 1.0

AusCERT

Australian Cyber Emergency Response Team

Questions?

AusCERT: membership@auscert.org.au

Phone: 1800 648 458

Mike Holm, Operations Manager, AusCERT

mike@auscert.org.au | 0417 440 189