Incident Handling and Response

Motivation

- Security incidents (violations) do happen!
- How do you minimise damage (disruptions)?
  - Coordinated
  - Consistent
  - Appropriately
  - Prepared
  - Timely
- Can we learn from them to prevent (better prepared) future events?

Think About

- How would you handle a incident?
- How would you prioritize the tasks required to handle the incident?
- What kinds of tools or skills would be required for analysis?
- If you need assistance, who would you contact?
- If contacted by the media what do you tell them?
- What are the post-incident activities you would do?

Incident Response

- The idea is to have a plan in place when (before) something BAD happens!
- NOT PANIC!

Why CERTs/CSIRTs?

- To be informed/notified
- To reduce impact of a security incident
- To understand the (root) cause
- Do something about it!

Be Notified

- How can others contact you?
  - Incidents
  - Source of incidents
  - Suspicious activities
  - Threat information
- WHOIS db
  - APNIC's Whois accuracy initiative

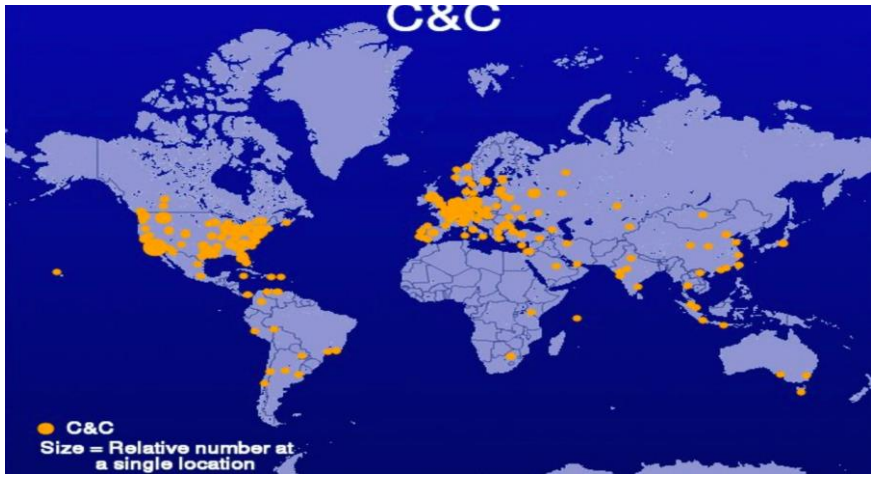
```
irt:            IRT-APNICTRAINING-AU
address:        6 Cordelia Street
address:        South Brisbane
address:        QLD 4101
e-mail:         training@apnic.net
abuse-mailbox:  training@apnic.net
admin-c:        AT480-AP
tech-c:         AT480-AP
auth:           # Filtered
mnt-by:         MAINT-AU-APNICTRAINING
changed:        abuse@apnic.net 20101126
changed:        hm-changed@apnic.net 20110624
source:         APNIC
```

Reduce potential impact

- Timeliness
  - No point wielding your sword once the enemy is gone
- Security incidents can affect
  - Business operation
  - Image/Brand
  - Safety
- Understand the (root) cause
  - Inform your community (constituents)

Do something about it

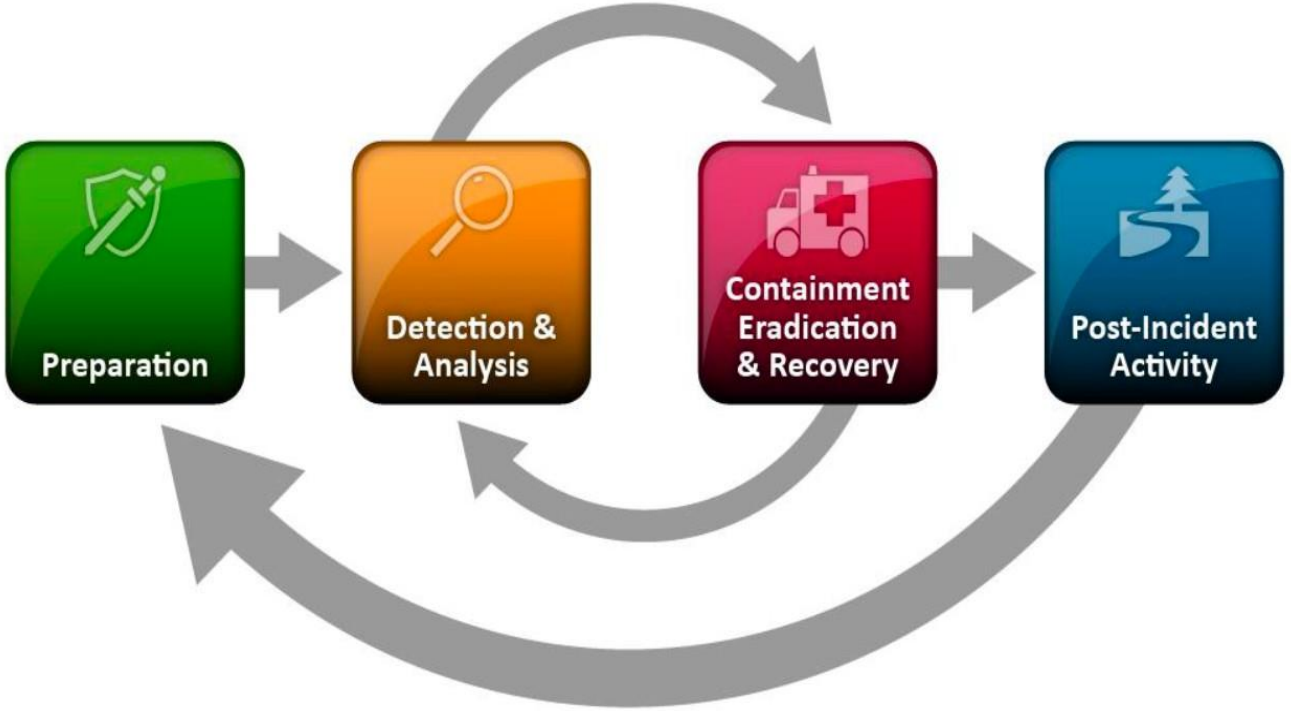
- Remediation
  - Analysis
  - Collaboration
  - Escalation
- DDoS example
  - Fixing
    - remove vulnerable hosts
    - remove vulnerable services
  - BCP38
    - source address validation
  - Continuous monitoring
- You are not alone
  - Join industry-wide initiatives



ShadowServer Foundation

CyberGreen

Incident response lifecycle



NIST: SP 800-61 rev2 (2012)

Preparedness

- Building and training an incident response team
  - SOPs and policies
  - Team
  - Communication (media)
  - Collaboration and cooperation

- Limit number of incidences
  - Secure (sufficiently) systems, networks and applications
  - Maintain timely backups
  - Make it difficult

Detection & Analysis

- Detect (potential) incidents
  - Anomalies
  - Understand expected versus observed
  - Log analysis
  - Seek expert opinion

- Understand the details
  - What kind of attack is it?
  - What is the potential impact?

Containment/Eradication/Recovery

- Limit (stop) the bleeding
  - Inform the community (constituents)
  - Isolate compromised systems/networks
    - Change DNS settings, filters/firewalls, disconnect
  - Collect evidence (for analysis)
    - Identify the attack host if
- Clean and restore operation
  - Learn how the attack was initiated
  - Remove breached accounts
  - Restore from backups
  - Patch identified vulnerabilities, change password, file permissions
  - Confirm system is functional

Post-Incident

- What lessons were learned
  - Discuss with your technical team and other organizations or parties who were involved
  - Did existing procedures help?
  - Can anything be improved?
  - How to prevent similar incidents in future?
    - Precursors or indicators to be watched for
- Share your lessons with the community
  - Your constituents
  - Other CERTs/CSIRTs
    - conferences

Summary

- Don’t Wait For a Security Incident!
  - How are you addressing Cyber Security in your organization?
- Review Incident Response & Handling Capabilities
  - Think of Some Scenarios
  - Policies & Procedures
  - Point of Contact
  - Collaboration / Co-operation with others
- Training & Learning More
  - CSIRT/CERT Conferences & Events
  - Best Practices Documents and Guidelines

Do you have a CERT/CSIRT?

- Connect with APNIC's experts to discuss more
  - Adli Wahid & Jamie Gillespie (Internet Security Specialist)
    - adli/jamie@apnic.net

Security Workshop in Bhutan (btCIRT)

Tonga CERT Discussion

References

- Recommended
  - RFC 2350 Expectations for Computer Security Incident Response
    - https://www.rfc-editor.org/rfc/rfc2350.txt
  - APCERT (Asia Pacific Computer Emergency Response Team)
    - http://www.apcert.org
  - Forum of Incident and Security Response Teams
    - http://www.first.org
  - European Union Agency for Network & Information Security
    - http://www.enisa.europa.eu/activities/cert
  - NIST.Gov
    - SP 800-61 (Revision 2) Incident Handling Guide
    - http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
  - Best Practice Forum @ IGF 2014
    - Establishing and Supporting Computer Emergency Response Teams (CERTs) for Internet Security http://bit.ly/11MwuCI


Questions