

AFP Summit on Enhancing Cyber Security  www.phcert.org

Cyber Security Incident Management

ANGEL S. AVERIA, JR.
 President, Philippine Computer Emergency Response Team
 Senior Security Consultant, Zylogix Systems Corporation

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Agenda

- Computer Security Incidents:
 - Global concern
 - Global response
 - Response in the Philippines
 - Incident Handling and Management

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Global Concern: A World Under Attack

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Web War I



- Estonia: World's most wired nation
- April 27, 2007: CyberAttack
- Denial of Service Attack
- Attack came from various servers from South America, Europe, Asia
- Swamped the websites of Estonia's private and public organizations

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Attacks

- Denial of Service
- Port Scans
- Ping of Death
- Malware Attacks
 - Trojans
 - Viruses
- Defaced or manipulated websites


National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Attack Vectors

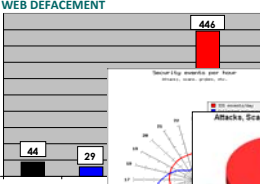
- Unwanted Email
 - Where/how do perpetrators get email addresses?
 - Ever received a PHISHING email?
 - How about Nigerian Scam?
- Unwanted SMS Message
 - Where do they get numbers?
 - Scams
- Instant Messaging
 - Social Engineering
- Attached Files
 - PDF, Executables, Documents

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

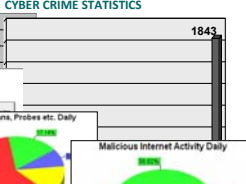
AFP Summit on Enhancing Cyber Security  www.phcert.org

Numbers tell the story

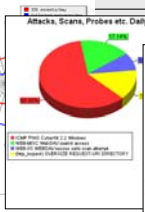
WEB DEFAACEMENT



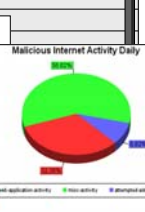
CYBER CRIME STATISTICS




Attacks, Scams, Probes etc. Daily



Malicious Internet Activity Daily



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

On the rise...

- Intruder techniques → sophistication
- Detection → difficult
- Identifying and catching perpetrators → greater challenge
- Damage:
 - Operational Disruption
 - Financial loss
 - Data confidentiality and integrity
 - Reputation and credibility

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Objectives

- Thrill
 - Challenge to break-in
- Financial gain
- Revenge
- Power
- Push political agenda
- Terrorism

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Global Response: CERTs / CSIRTs

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

CERT? CSIRT?

- CERT = Computer Emergency Response Team
- CSIRT = Computer Security Incident Response Team

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

The Geeky Side

- Artifact analysis
- Malware analysis
- Vulnerability analysis
- Network monitoring
- Technology research

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Beyond Techy

- Incident Handling and Management
- Awareness and Education
- Alerts and Advisory
- Coordination
- Policy Development

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Asia Pacific CERT

Economies Covered




- Australia
- Bangladesh
- Brunei
- China (PROC)
- Chinese Taipei
- Hong Kong
- India
- Indonesia
- Japan
- Korea
- Malaysia
- Philippines
- Singapore
- Sri Lanka
- Thailand
- Vietnam

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Computer Security Incident Response in the Philippines

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

About PhCERT

- A member of APCERT
- Point of Contact
- Coordination with other CERTs/CSIRTs
- Incident handling and Management
- Information dissemination
- Pass on Alerts, warnings, and advisories
- Awareness and Education
- Policy Development
 - Legislative support
 - Rules and regulation development
- Coordination with Law Enforcement

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Challenges

- Resolve incidents at the shortest time possible
- Prevent/avoid the occurrence of such incidents
- Mitigate impact and minimize damage

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Information Security Practice in the Philippines

- Certified information security professionals
- Organizations maintain information system security teams

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10




AFP Summit on Enhancing Cyber Security


www.phcert.org

Why Create CERTs/CSIRTs

- Best practice
 - Obligation to stakeholders
- Protection of the organization
- Information Gathering
- Incident coordination

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security


www.phcert.org

Why Create CERTs/CSIRTs

- Quickly respond to security incidents
- Quickly resolve security breaches
- Promote information security awareness, discipline, and practice

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security


www.phcert.org

Why Create CERTs/CSIRTs

Preparedness and adopting an information security culture are keys to protecting our most valuable information assets.

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security


www.phcert.org

Incident Handling and Management



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security


www.phcert.org

Incident Handling and Management Process and Practice

- Prepare
 - Gather information
 - Vulnerability Information
 - Security Reports, Bulletins, and Alerts
 - Reports on malicious activities
 - Malware information



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security




www.phcert.org

Incident Handling and Management Process and Practice

- Protect
 - Firewalls
 - Intrusion Prevention Systems
 - Intrusion Detection Systems
 - Harden systems and applications
 - Update and apply patches




National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security




www.phcert.org

Incident Handling and Management Process and Practice

- Monitoring
- Detection
- Response
- Resolution




National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security


www.phcert.org

Incident Handling and Management Process and Practice

- 3C Framework
 - Cooperate
 - Collaborate
 - Coordinate
- Document



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security




www.phcert.org

Incident Handling and Management Monitoring

- Gather information
 - Vulnerability Information
 - Security Reports, Bulletins, and Alerts
 - Reports on malicious activities
 - Malware information
- Keep watch



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10


AFP Summit on Enhancing Cyber Security


www.phcert.org

Incident Handling and Management Detection

- Network Monitor
 - Anomalous activities
 - Unusual traffic
- Intrusion detection system
- Incident report

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10



AFP Summit on Enhancing Cyber Security


www.phcert.org

Incident Handling and Management Response

- Triage
 - Identify
 - Categorize
 - Prioritize
- Escalate

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10



AFP Summit on Enhancing Cyber Security


www.phcert.org

Incident Handling and Management Resolution

- Known incident: execute appropriate response
- Unknown → Escalate to Malware Analysis
 - Capture
 - Analyze
 - Develop response
 - Resolve


National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Incident Handling and Management 3C Framework

- Cooperate
- Collaborate
- Coordinate
- Request and exchange information with other CERTs/CSIRTs
- If host is in other jurisdiction, request CERT/CSIRT in that jurisdiction for assistance


National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

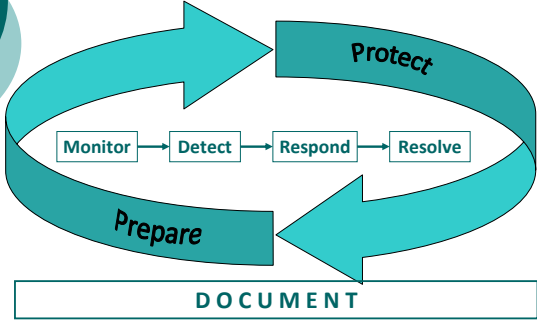
Incident Handling and Management Document

- Incident ticketing system
 - Monitor / track incidents until resolution
- Keep / hold in database
 - Incident type, description, class, priority
- Keep record of analysis
- Templates
 - Acknowledging reports
 - Request for information
 - Bulletins, Alerts

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Incident Handling and Management



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

Incident Handling and Management Some Tools of the Trade



National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10

AFP Summit on Enhancing Cyber Security  www.phcert.org

For more info: info@phcert.org

Maraming Salamat Po!

National Cyber Defense Capability Development Conference | Dusit Thani Manila | 03/10-11/10