The Value Proposition in a Pacific CERT
Outline

• Background (who and what)
• Services- In Depth
• Reason and Cause
• Conclusions
PACCERT’s New Core Services

- Priority Incident Response
- Malware Analysis
- Security Audit (Penetration Testing)
- Training
- Remote Monitoring
- Conferences
- Priority Alerts
- Research
Target Beneficiaries

• **22 Pacific Island countries**

• Within these countries, constituents will be drawn from the following sectors:
  - Government IT departments
  - Tel-Co and ISPs
  - Financial Service Providers
  - Essential Service providers
  - Non-Goverment organizations
  - Large Organizations
  - SMBs
  - Others as may be decided on a case by case basis
What is IR?

• IR is the process of handling CSI
  • Detecting and Analyzing the incident
  • Mitigating the damage

• The goals of IR service is to:
  • Cease the incident
  • Recover the infected systems to normal state
  • To understand how it happened and to prevent further occurrences or damages
IR Typical Activities

- Receive Incident reports from inside and outside our constituency, and coordinate to handle the incidents
- Sharing and exchanging incident related information with internal and external parties
- Notifying incidents to relevant organizations
  - Take down malware distribution sites
  - Take down phishing sites
  - Notify the admins of defaced websites
  - others
Incident Response and Handling Service - Types

- **Offsite or Remote Response**
  - PACCERT Staff will respond to incident reports and provide assistance to stakeholders via telephone or email support. PACCERT staff will typically not have access to any of the target systems but will relay ‘suggestions’ to the onsite admins.

- **Onsite Response**  
  - PACCERT staff will respond to incident reports and provide assistance to stakeholders in person at the site. PACCERT staff may be granted temporary administrator status in the target systems to facilitate investigation, containment and eradication if necessary.

  **NOT YET IMPLEMENTED**
Examples of CSI (1/2)

- Scan activity to servers
- Web defacements
- Information leakage
- Phishing sites
  - Using servers for phishing sites
  - Using websites for phishing sites
- Intrusion (web, database, FTP, proxy, etc...)
- DOS attacks to web servers
- Using proxy servers as open proxy
- SMTP relay
- Virus infections
Examples of CSI (2/2)

- Forged emails returning large amount of errors mails
- Malware distribution
- Bot infections
- One-click fraud
- Operational errors
- SPAM
- Targeted attacks
- Hactivism
Incident Response - Roles

**HANDLER**
Checks inbox. Triage and verify Reports. Issues *Call-for-close*.

**REVIEWER**
Verify Draft notifications. Send notifications.

**CLOSER**
Verify *Call-for-close*. Close Incidents.
Incident Response (IR) Service Workflow - Overview

1. Receive
2. Triage
   - NOT an incident report
   - Incident report
3. A1. Issue a report ticket
4. A2. Auto reply
5. A3. Confirmation of receipt
6. A4. Feedback to the reporter
7. A5. Close the report
8. B1. Issue an incident ticket
9. B2. Decide if incident notification is necessary
   - YES
   - B2. Decide if incident notification is necessary
   - NO
   - B3. Close the incident
10. C1. Issue an incident notification ticket
11. C2. Notify
12. C3. Assess the threat
   - Threat identified
   - No threat
13. C4. Close the notification

Spam Trash

Incident Response (IR) Service Workflow
IR Workflow – by Roles

(RE1) Report /request

incident@paccert.org

(RE2) Retrieve emails

(RE3) Triage

(H1) Create Incident Ticket(s) and coordination

(H2) Drafting

(RW1) Review the draft

(RW2) Send the email

(C1) Confirmation of ‘cfc’

(C2) Close the incident

Incident continues?

YES

NO

(I) Receipt

Handling

Review

Closing

(H3) Change to ‘cfc’
Malware 101

- **MALicious SoftWARE**
  - is an all encompassing concept and includes viruses, worms, Trojans, rootkits, bots, etc...
- Purpose
  - Mischief
  - For profit
  - National agendas?
- Trends
  - Evolution towards more targeted attacks
  - “It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.” – Sun Tsu
What is Malware Analysis

• “The goal of MA is to determine how a specific piece of malware functions, so that defenses can be built...” – SANS

• Malware Analysis seeks to answer 2 Questions:
  1. How did this machine get infected?
  2. What does this malware do?
PACCERT Secure Environment

- Need for secure environment to conduct investigation
  - Prevent the propagation of malware
  - Allow for through analysis

- This is done through the use of Special equipment
  - Snapshots (Deep freeze and VM-Ware)
  - DMZs and other network isolation strategies
  - Rigid procedures
Types of Malware Analysis

• 3 Types of Analysis:
  - Surface Analysis
  - Runtime Analysis
  - Static Analysis

Useful Information

Time Required to perform

Difficulty
Malware Analysis Workflow Overview

Start

Surface Analysis

- Enough?
  - Yes
  - No

Runtime Analysis

- Enough?
  - Yes
  - Summarize Result
  - End
  - No

Static Analysis

- Summarize Result
- End
Surface Analysis

- Surface analysis consists of recognizing or discovering a malware's signature, or other identifying characteristics and gathering information based on this information.
Surface Analysis workflow

1. Preparation
   - P1. Environment Setup
   - P2. Tool Setup

2. Pack Analysis
   - X1. Packer Check
     - Packed?
       - No
       - Yes
         - Is trusted tool available?
           - No
           - Yes

3. Comparative Analysis
   - C1. Existing Analysis Result
   - C2. Virus Scan
   - C3. Public Information

Save Result

END
Runtime or Dynamic Analysis

- Dynamic or Runtime analysis involves the running or executing of the target sample and gathering diagnostics and behavior results based on logs and monitoring tools.
Runtime Analysis Workflow

START

R0. Prepare Environment

R1. Start Information Capture Tools

R2. Establish a 'before' snapshot

R3. Execute Malware

R4. Compare Before and After

R5. Check communication logs

Enough?

Yes -> END

No -> R5. Check communication logs

END
Static Analysis or Reverse Engineering

- Involves the examination of the machine code of the binary sample in order to further discover functionality and techniques used by the sample.
Hierarchy of programming languages

- Scripting/Interpreted Languages
  - Perl, Python, Shell, Java
- High/Middle Level Languages
  - C, C++
    - (What Most Malware Is Written In)
  - Assembly Language
    - Intel x86, etc.
      - (First Layer of Human Readable Code)
  - Machine Code
    - Hexadecimal representations of Binary Code Read By The Operating System
  - Binary Code
    - Binary code read by hardware
      - Not Human Readable

Flow of Compilation and Disassembly
Static Analysis Workflow

- T0. Prepare Environment
- T1. Information Collection
- T2. Preparation to read the Code
- T3. Read the Code
- T4. Summarize Findings

START → T0. Prepare Environment → T1. Information Collection → T2. Preparation to read the Code → T3. Read the Code → T4. Summarize Findings → END
The Global Cost of Cybercrime

$97M
Fake Anti-Virus

$10M
Stranded Traveler Scam

$200M
Fake Escrow

$1B
Advanced Fee Fraud

$370M
Online Banking Fraud

$3.4B
Anti-Virus

$1B
Bank counterm easures

$320M
Phishing

$1B
Patching Vulnerabil ities

$10B
Cleanup

Source: “Measuring the Cost of Cybercrime,” by Ross Anderson, University of Cambridge; Chris Barton, Cloudmark; Rainer Böhme, University of Münster; Richard Clayton, University of Cambridge; Michel J.G. van Eeten, Delft University of Technology; Michael Levi, Cardiff University; Tyler Moore, Southern Methodist University; and Stefan Savage, University of California, San
How can you leverage PACCERTs services?

• Include PACCERT in DR and IR procedures.
  • Does your Organization have a DR or IR procedure for CSI?

• Received a scam or phishing mail?
  • Send it to us at incident@paccert.org. We will work to shut down scam and phishing sites targeted at our constituents

• Really, how can YOU leverage PACCERTs services?
  • You are in the best position to answer that question, so please talk to us.
Vinaka Vakalevu