Building a Research and Extension Center

VAN OWEN M. SESALDO
Cybersecurity Research and Extension Center
University of the Philippines Cebu
Motivation

Google Search Console

Hacked content detected on http://upcebu.edu.ph/

To: Webmaster of http://upcebu.edu.ph/,

Google has detected that your site has been hacked by a third party who created malicious content on some of your pages. This critical issue utilizes your site's reputation to show potential visitors unexpected or harmful content on your site or in search results. It also lowers the quality of results for Google Search users. Therefore, we have applied a manual action to your site that will warn users of hacked content when your site appears in search results. To remove this warning, clean up the hacked content, and file a reconsideration request. After we determine that your site no longer has hacked content, we will remove this manual action.

Following are some example URLs where we found pages that have been compromised. Review them to gain a better sense of where this hacked content appears. The list is not exhaustive.

http://upcebu.edu.ph/where-to-buy-viagra-melbourne/

Here's how to fix this problem:

1. Use the examples provided in the Security Issues report of Search Console to get an initial sample of hacked pages.
Motivation

http://upcebu.edu.ph/where-to-buy-viagra-melbourne/

• Logs show frequent access from IP address with *whois* info tracing back to AU

• A week later, office received an email from an AU-based security provider telling me our website was vulnerable
Motivation

• Several conclusions can be drawn for the information

• Wrong conclusions can lead to a lot of trouble

• How do we get the right conclusions?
Motivation

• Are we the only one who experience this?

• What about the non-tech people – our end users?
Motivation

Public school teacher in debt because of identity theft

Published February 26, 2016 10:48pm

A public school teacher may be a victim of identity theft as he owes three banks P800,000 for loans he did not apply for, according to a report by John Consulta on GMA-7’s “24 Oras” on Friday.
Motivation

2 out of 10 Aware of dangers

Quick survey conducted for public, with a barangay as sample
Motivation

Know how to run IT departments

Quick survey conducted with a barangays as sample
Motivation

23% Know how to secure

Quick survey conducted with a barangays as sample
There are a lot of courses for technical people.

How about the non-tech?
We have to do something!
I mean all of us 😊
Timeline
- Applied for a grant for training staff - 2015
- Application got to final stages but failed – 2016
- Applied for grant from another agency – 2016-2017
- January 2018 – given an equipment grant by DOST for the creation of:
  University of the Philippines Cebu Cybersecurity Research and Extension Center

Problems:
Resources
Lack of Education
Lack of Urgency
Goals

Academic Goals
- Program Creation / Enhancement
- Contribution to BOK

Community Goals
- Creation of CSIRT / SOC
- Social Relevance
Relevance

• Contribute to nation building – more security professionals

• Run public info campaigns – extract socially relevant materials from academic work

• Channel for public to ask help for cybersecurity incidents

• Assist with law enforcement (long term)
Developing Research Areas

- SDN Security Controllers
- Secure applications
  - Privacy-by-design principles
- Cryptography (mid term)
- ML x Security (mid term)
- VR x Security (mid term)
- Blockchain (mid term)
- Network security – malware (long term)
Community Coals

Developing Capacities

- CSIRT
  - Forming a team
  - Help from the community
  - Gathering contacts for collaboration

- Public learning platform
  - Information campaigns for the public
Phases

- Cyber Range
- VAPT Center (apps and network)
- Malware Analysis Center
- Security Operations Center
Current Phase

Phase 1: Cyber Range
Cyber Range Setup

- Sandboxed environment
- One rack for virtualization
  - Firewalls, routers, servers, etc
- NGFW mainly for threat visualization
- 12 - seats for red/blue simulations (Open Cyber Challenge Platform - NIST)

- Facility for public training

- Team with pleasing personalities 😊
Collaborations

- Connect with your CSIRT

- Conduct joint security-related exercises

- Hosting academic programs from other universities in UP Cebu

- Engage in exchange student programs

- Assist your organizations in conducting trainings in UP Cebu or in Cebu
University of the Philippines Cebu
Cybersecurity Research and Extension Center

VAN OWEN M. SESALDO
vmsesaldo@up.edu.ph

Thank you!