Agenda

• About HKIRC
• Company Mission
• Security Challenges & Prevention
  • Phishing attack
  • Ransomware
  • Data Breaches
• Security Measures
• Conclusion
About HKIRC

• Non-profit member-based organisation
• Set up in December 2001
• Endorsed by the Government of the HKSAR
• Oversee the administration and assignment of the country code top level Internet domain names ending with .hk and 香港.
Company Mission

Mission

• Providing, and supervising the provision of .hk and 香港 Internet domain names registration, resolution and related services in an uninterrupted, effective, customer-centric and sustainable manner.

• Promotes Hong Kong as an inclusive, secure, innovative and international city for the Internet and encourages the use of Internet and the related technologies.
Cyber Security Schools Audit 2019 in UK

- LGfL (London Grid for Learning) & NCSC (National Cyber Security Centre, part of GCHQ) carried out a joint audit of cyber security in schools across the UK
- The audit was open from 15 March – 20 April 2019
- 432 schools took part
- Findings were discussed vastly in media
- Issues highlighted in the report may also applicable in schools in HK
83% of schools experienced different levels of cyber-incidents

- Fraudulent emails sent to staff or staff directed to fraudulent websites
- Important information made unavailable, whether short-term or permanently
- Malware infection including viruses or ransomware on any network-connected equipment
- Unauthorised (including accidental) PUPIL use of computers, networks or servers
- People impersonating your school emails
- Attempted attacks to take down your website or online services (successful or otherwise)
- Unauthorised (including accidental) STAFF use of computers, networks or servers
- Any other cybersecurity breach or attack
- Important school information changed without permission
- Unauthorised (including accidental) EXTERNAL use of computers, networks or servers
- Leaks of confidential information from an online system
Highlight of Findings (Cont’)

• 98 and 99 percent of schools, respectively, had antivirus and firewall protections

• 85 percent of schools had a cyber security policy or plan, but only 45 percent included core IT services in risk register & only 41 percent had a business continuity plan

• Only around a third of schools (35 percent) train non-IT staff in cybersecurity

• Less than half of schools (49 percent) were confident that they are adequately prepared in the event of a cyberattack

• A focus on support for non-IT staff is a clear need, 92 percent of schools welcome more cybersecurity awareness training for staff
Common Attack in Schools
Phishing Attack
Recent Phishing Attacks
Recent Phishing Attacks (Cont’)

From Inland Revenue Department <taxinfo@ird.gov.hk>

Subject: TAX INFORMATION UPDATE.

To: undisclosed-recipients:;

ATTENTION:

2018-19 Budget – Tax Measures

In his 2018-19 Budget, the Financial Secretary proposed a number of tax measures, all of which require legislative amendments before implementation.

Reducing profits tax, salaries tax and tax under personal assessment for the year of assessment 2017/18

Adjusting the tax bands and marginal tax rates.

Increasing allowances and introducing a personal disability allowance.

Raising the deduction ceiling for elderly residential care expenses.

Relaxing the requirement for election of Personal Assessment by married persons.

Kindly update your tax information with the inland revenue department from the attached pdf.

Regards,

Inland Revenue Department

1 attachment: UPDATE-TAX.pdf size unknown
Recent Phishing Attacks (Cont')
Recent Phishing Attacks (Cont’)
Recent Phishing Attacks (Cont’)

From Inland Revenue Department <egis_notification@ogcio.gov.hk>

Subject Refund Account - 200013364790

To [Redacted]

Reply To: "e alert" <aler12@ird.gov.hk>

Wednesday, February 28, 2018 06:45 AM

We are sending this email to announce that after the last annual calculation of your fiscal activity, we have determined that you are eligible to receive a tax refund of 1917.35 HKD.

In order to receive your tax return online

[Redacted]

This mail is system-generated, please do not reply to this email account.

CONFIDENTIALITY
This email message (together with any attachments) is intended solely for the use of the designated recipient. It may contain confidential information that is privileged. If you are not the intended recipient, you should not
Recent Phishing Attacks (Cont')
re: "[redacted]"

to me  

I know, [redacted], is your pass word. you may not know me and you are most likely thinking why you’re getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What exactly did I do?
I created a double-screen video. First part displays the video you were watching (you’ve got a good taste lol), and 2nd part displays the recording of your web cam.

Exactly what should you do?
Well, I believe, $1200 is a fair price for our little secret. You’ll make the payment through Bitcoin (if you don’t know this, search “how to buy bitcoin” in google).

BTC ADDRESS: 1JCh[redacted]byFJbu7
(It’s CASE sensitive, so copy and paste it carefully)

Note:
You have one day to make the payment. (I’ve a specific pixel in this message, and right now I know that you’ve read this e-mail). If I do not receive the Bitcoins, I will certainly send out your video recording to all of your contacts including friends and family, colleagues, and so forth. nonetheless, if I receive the payment, I’ll destroy the video immediately. If you need proof, reply with "yes!" and I definitely will send your video recording to your 14 friends. It is a non-negotiable one time offer, thus don’t ruin my time & yours by responding to this e-mail.
Tackling Phishing Attack

• Do not open suspicious links in E-mail & Web browser
• Do not key-in user name and passwords from forms open by E-mails
• Make sure system patches and anti-virus software are up-to-date
• Enable Two Factor Authentication (2FA) function wherever it is provided
Ransomware
Ransomware is a serious security threat that limits victims to access their files or system functions. It has “data-kidnapping” capabilities.

Cybercriminals tend to threaten victims to pay ransom (bitcoin) in order to regain access to their files or systems.

Cybercriminals

2016 Locky, Zepto, CryptXXX
2017 WannaCry, NotPetya
2018 GandCrab, SamSam
2019 LockerGoga, etc.
Ransomware Evolution

Crypto Ransomware
- 2013 CryptoLocker (PC)
- 2014 BitCrypt (PC)
- 2014 CryptoDefense (PC)
- 2014 Synolocker (NAS)
- 2014 Simplocker (Mobile)
- 2014 CryptoGraphic Locker
- 2015 CryptoWall, TeslaCrypt, CTB-Locker
- 2016 Locky, Zepto, CryptXXX
- 2017 WannaCry, NotPetya
- 2018 GandCrab, SamSam
- 2019 LockerGoga, etc.

Expect to continue ...
Newest Trend of Ransomware

**New Virus Decides If Your Computer Good for Mining or Ransomware**

Cryptojacking - secret use of your computing device to mine cryptocurrency.

CPU Surged During Cryptojacking
Suggestions to Defense Against Ransomware

• Do not pay cyber criminals ransom
• Do not open suspicious links in E-mail & Web browser
• Make sure system patches and anti-virus software are up-to-date
• Protect your data – backup your data regularly and put them offline
Data Breaches
Data Breaches Cases Surged since 2018…

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

Mr Gan Kim Yong
Assistant Minister for Health

About 1.5 million patients, including Prime Minister Lee Hsien Loong and a few ministers, have had their personal data stolen. Some 38,000 people also had their outpatient prescriptions stolen.
Data Breaches Cases Surged since 2018…
And Even in 2019…

British Airways faces $230m fine for data breach

By Adam Savitaro New York Times, July 8, 2019, 7:31 p.m.

LONDON — British authorities said Monday that they intend to order British Airways to pay a fine of nearly $230 million for a data breach last year, the largest penalty against a company for privacy lapses under a new European data protection law.

Hong Kong schools fall victim to cyberattack, raising fears for private data of pupils

South China Morning Post | Danny Mok danny.mok@scmp.com

Police investigating after eight schools are hacked, three of which report data leaks

Pupil addresses among information stored on administration system targeted by hackers

Three out of eight schools targeted have reported falling victim to data leaks after a government IT system was hacked. Photo: Shutterstock
Why Data Breaches?

Data Breaches are result of:

• Poor IT operational practices (e.g. late decommission of servers)
• Application vulnerabilities
• Advanced Persistent Threat (APT)
• Deficiency in outsourcing management
• Etc.

Organizations need to have a holistic security strategy – combining people, process and technology to reduce exposure to current & future attacks
Security Measures
Security Measures

• Security Measures can be classified into 3 categories: Technology, Process and People
Well planned Security Architecture needed:

- Anti-malware
- Firewall
- Network Access Control
- Encryption
- Patches update
- A lot more…
Well planned processes and procedures needed:

- IT and Security Policy
- Information Classification
- Risk Assessment
- A lot more…
Information Security Protection via People

People is the weakest link in cybersecurity, need more emphasis:

- Minimum Privilege and Accountability
- Password Management
- Security Awareness – avoid phishing & social engineering
- A lot more…
Conclusion

• Everyone relies on the cyber World to conduct business nowadays

• However, the cyber world is full of cybersecurity challenges

• We discussed some security challenges here:
  • Phishing Attack
  • Ransomware
  • Data Breaches

• To deal with these challenges, we need a holistic security strategy combining **people**, **process** and **technology**.

• Among these 3 aspects, **people** is the weakest link. More awareness effort needed.
Free In-Depth Website Security Scan

• In-Depth Website Security Scan now open for application
• All .hk users and HK SMEs can apply for the free service
• HKIRC will provide:
  • Remote black-box vulnerability scan for web server
  • Organized report for identified issues & mitigation actions
  • A consultation session for briefing report
  • Referral to appropriate solution vendors if needed
• Application form: [https://www.hkirc.hk/upload/blog/6/self/5df2ebec9c9e7.pdf](https://www.hkirc.hk/upload/blog/6/self/5df2ebec9c9e7.pdf)
• Any inquiry, please call HKIRC hotline 2319 2030 or E-mail to sme-security-scan@hkirc.hk
In-depth Webscan for SME

HKIRC → Custom made → Security scan report

Vulnerability scan → .hk website

Face-to-face session

Attack
Sample Report

All Rights Reserved.
Hong Kong Internet Registration Corporation Limited

Technical Summary

<table>
<thead>
<tr>
<th>Section</th>
<th>Risk Level</th>
<th>CVSS*</th>
<th>Issue</th>
<th>Summary of Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>SQL Injection</td>
<td>SQL injection may be possible</td>
<td>Modify program logic to filter input properly</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Cross Site Scripting (Reflected)</td>
<td>Cross-site scripting (XSS) is an attack technique that involves echoing attacker-supplied content into a user’s browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within VisioClip, an RSS reader, or an email client.</td>
<td>Modify program logic to filter input properly</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>X-Frame-Options header Not Set</td>
<td>X-Frame-Options header is not included in the HTTP response to protect against Clickjacking attacks</td>
<td>Ensure web server sets the X-Frame-Options header appropriately and X-Context-Type Options header set to 'strict' for all web pages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Web Browser XSS Protection Not Enabled</td>
<td>Web Browser XSS Protection is not enabled or configured correctly</td>
<td>Turn off X-Frame-Options HTTP response header to 'strict'</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>X-Content-Type-Options Header Missing</td>
<td>The X-Content-Type-Options header X-Content-Type-Options was not set to 'strict'. This allows some older versions of browsers to Bypass content sniffling on the response body.</td>
<td>Ensure web server sets the X-Frame-Options header appropriately and X-Context-Type Options header set to 'strict' for all web pages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Absence of Anti-CSRF Token</td>
<td>No Anti-CSRF tokens were found in a HTML submission form</td>
<td>Generate unique form for each form</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Cookie No httpOnly Flag</td>
<td>A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can run on this page then the cookie will be accessible and can be transmitted to another site. If more than a session cookie then session hijacking may be possible.</td>
<td>Ensure HttpOnly flag is set for cookies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Disclaimer

A remote web vulnerability assessment was conducted by HKIRC against the web-interfaced system. The purpose of this assessment was to remotely identify and quantify vulnerabilities or potential threats in the web-interfaced system before they are exploited by attackers. This report is provided as it is, and HKIRC cannot guarantee all vulnerabilities of the system are identified in this remote security scanning.

1 The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and provide a numerical score reflecting its severity. CVSS is a published standard used by organizations worldwide, and the HKIRC is in the process of improving it.

Background

A remote web vulnerability assessment was conducted by HKIRC against the web-interfaced system. The purpose of this assessment was to remotely identify and quantify vulnerabilities or potential threats in the web-interfaced system before they are exploited by attackers. This report is provided as it is, and HKIRC cannot guarantee all vulnerabilities of the system are identified in this remote security scanning.

Executive Summary

This security scan identified 2 High severity issues, 1 Medium severity issue and 4 Low severity issues. Most issues can be rectified by modifying configurations of web server. Others may need a review on application logic.

See below for analysis of these items. For technical details, please refer to the Appendix Section.

Findings and Recommendations

Findings

- The system seemed to be a shared web hosting. So only web application contents are scanned in this assessment, instead of running a full security scan on the server.
- The major issue of the website is that user input is not filtered properly. It is possible to inject scripts and even SQL statements in user input variables and cause it executed by the server.
- Other issues are related to configuration of web server

Recommendations

- Filter user input properly. Remove special characters like '<', '>', '@', '#', '%', '*', ' ', '"', and other special characters from user input
- Configure web server to enable security related headers and settings
Q & A