Latest Cyber Security Threats & Trends
The Ways To Deal With Them
Summ CHAN | Security Consultant | September 2019
Agenda

• Latest Cyber Security Threats & Trends
• Cyber Attack & Defense
• Security Incidents Handling
• Security Advice Round Up
Hong Kong Computer Emergency Response Team Coordination Centre
(香港電腦保安事故協調中心)

Mission:
As the **Centre for coordination** of computer security incident response for local enterprises and Internet Users, and the **International Point-of-Contact**

- Founded in 2001
- Funded by Government
- Operated by Hong Kong Productivity Council
HKCERT services

01 Security Alert Monitoring and Early Warning
02 Report and Response
03 Publication of Security Guidelines and Information
04 Promotion of Information Security Awareness
Cyber Security

Threats & Trends
Summary of HKCERT Security Incident Reports

YoY ↑ 55%

Referred case contributed 95%
Summary of HKCERT Security Incident Reports

- **Botnet** (殭屍網絡): 37%
- **Malware** (惡意軟件): 32%
- **Phishing** (網絡釣魚): 21%
- **Defacement** (網站塗改): 1%
- **DDoS** (分散式阻斷服務攻擊): <1%
- **Others** (其他): 9%

Total: 55%

Source: HKCERT
Cyber Attack & Defense
#Cyber_Attacks
Phishing
What is Phishing?

1. Attacker sends an email to the victim
2. Victim clicks on the email and goes to the phishing website
3. Attacker collects victim’s credentials
4. Attacker uses victim’s credentials to access a website

Legitimate Website

Phishing Website

Attacker

Victim
Cyber Security Incidents of Enterprises in Past 12 Months (2019-03)
350 Large Enterprises and SMEs interviewed

### Top 5 External Attacks

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Incidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Email</td>
<td>77% (+28%)</td>
</tr>
<tr>
<td>Ransomware</td>
<td>42% (-10%)</td>
</tr>
<tr>
<td>Other Malware Attack including Botnet</td>
<td>22% (-3%)</td>
</tr>
<tr>
<td>CEO Scam</td>
<td>18% (-17%)</td>
</tr>
<tr>
<td>DDoS</td>
<td>14% (+4%)</td>
</tr>
</tbody>
</table>

Source: SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2019, HKPC
Cyber Security Incidents of Enterprises in Past 12 Months (2019-03)

Industries Most affected by Island Hopping

- Finance: 47%
- Manufacturing: 42%
- Retail: 32%
- Healthcare: 21%

- Hop to connected network (enterprise internal) – lateral movement
- Reverse Business Email Compromise – take over mail server (enterprise internal)
- Website waterhole (trap customers)

Source: Global Incident Response Threat Report, 2019-Q1, Carbon Black
PHISHING . . .
the begin of a cyber attack story

The information is then used to access important accounts and can result in identity theft and financial loss.
Phishing Tactics: New Developments (1)

- Domain Spoofing
  - Fake Domain: e.g. "zhongyinhk.com" used to phishing BOCHK
  - Punycode Domain

- Use of HTTPS

  "Use of HTTPS (APWG 2019 Q1 Report)"

  58% of phishing using HTTPS (APWG 2019 Q1 Report)
Phishing Tactics: New Developments (2)

- **Multi-level Social Engineering**
  - Attacker created a post in LinkedIn and built trust on the post with comments and dialogue with the “friends” for some time.
  - Attacker sent email to victim with reference to the post

- **Evade spam filter by using image**
  - Ransom email in image
  - Payment bitcoin address in QR code

**Fraudsters deepfake CEO’s voice to trick manager into transferring $243,000**

by RAVIE LAHSHMANAN — 9 days ago in SECURITY
How To Distinguish PHISHING SCAM
<table>
<thead>
<tr>
<th>Email Subject</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Check Required Immediately</td>
<td>19%</td>
</tr>
<tr>
<td>Your Order with Amazon.com/Your Amazon Order Receipt</td>
<td>16%</td>
</tr>
<tr>
<td>Announcement: Change in Holiday Schedule</td>
<td>11%</td>
</tr>
<tr>
<td>Happy Holidays! Have a drink on us.</td>
<td>10%</td>
</tr>
<tr>
<td>Problem with the Bank Account</td>
<td>8%</td>
</tr>
<tr>
<td>De-activation of [[email]] in Process</td>
<td>8%</td>
</tr>
<tr>
<td>Wire Department</td>
<td>8%</td>
</tr>
<tr>
<td>Revised Vacation &amp; Sick Time Policy</td>
<td>7%</td>
</tr>
<tr>
<td>Last reminder: please respond immediately</td>
<td>6%</td>
</tr>
<tr>
<td>UPS Label Delivery 1ZBE312TNY00015011</td>
<td>6%</td>
</tr>
</tbody>
</table>

Source: [https://www.securitybrigade.com](https://www.securitybrigade.com)
GREED

CURIOSITY

URGENCY

FEAR
How to distinguish Phishing Scams?

Sample 1

Lucky Draw & Rewards

URGENCY

GREED
How to distinguish Phishing Scams?

Sample 2

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To: 
Subject: Your Mailbox Will Shutdown Verify Your Account

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

Verify Now

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved
How to distinguish Phishing Scams?

Sample 3

**Banking & Finance**

**Retail**
How to distinguish Phishing Scams?

Sample 4

- NO HTTPS
- FAKE DOMAIN
- URGENCY
How to distinguish Phishing Scams?

Sample 5

Internet Service Provider

Enter the URL on your own

Fear

HTTPS
How to distinguish Phishing Scams?

Sample 6
Protection against Phishing Attacks

- Think before you click
- Pick up the phone to verify
- Use two-factor authentication (2FA) across all accounts
- Use different passwords for different services
- Use email filtering technology & make sure the technique is up-to-dated
- Conduct phishing drill exercises for all general staff
Malware | Propagation Channels

**Executable**
- Fake security software / mobile app
- Fake video player codec

**Document Malware** ★
- Embedded malware in PDF or Office files
- Botnet served PDF malware

**Website ★★★**
- Legitimate and trusted websites compromised
- Web admin incapable to detect and mitigate the risks
Multi-Stage Malware Infection | Drive-by Download

- Exploits imported from other servers via iframes, redirects
- When compromised, dropper download and install the actual bot malware

1. Web request
2. Redirected to Exploit Server
3. Serve exploit page
4. Redirected to Malware Server
5. Download Malware

Image credit: Flaticon.com
Botnet (roBot Network)
Infrastructure of Controlled Victim Computers (BOTs)

Bot Herder

C&C

Up: Data
Down: Command/Update

bot

Up: Data
Down: Command/Update

bot

bot

bot

bot

bot

bot

Spam, Malware & Phishing

victim

victim

DDoS Attack
Ransomware

Untargeted attack
Pay 2 Bitcoins ransom

Targeted attack; Time-bomb
Ransom based on company size (from 2 to 400 BTC)

Pay ransom to get your DATA back

Pay ransom on time or your DATA is DESTROYED

Doxware

Pay ransom on time or your DATA is PUBLICIZED

Popcorn time

Jigsaw

Pay ransom or INFECT 2 friends to get DATA back
Protection against Ransomware

- Isolate infected computer immediately
- Do NOT pay ransom nor contact attacker
- Perform regular backups on important data and keep an offline copy
- Ensure that OS, software and anti-virus signatures are kept updated regularly
- Do NOT open suspicious email attachments and website links
ANYTHING Can Be Targeted [video]

• Crime-as-a-Service
• Launch of cyber attacks are much easier than we can think of nowadays!

• Are you ready to face all these challenges?
Security Incidents Handling
Incident Reporting Basics (1)

**WHAT**
- What actually happened?
- What the incident might mean for the organization?
- What is the impact?
- What system affected?
- What service affected?
- What actions had been taken?
- and etc.

**WHO**
- Threat actor / IP address
- Attack source
- Hacking group
- Attack target
- Owner of targeted system
- Owner of involved business function
- Customers affected
- Parties involved
  - Internal
  - External
- and etc.
Incident Reporting Basics (2)

**WHEN**
- When the incident happened?
- When the incident being detected?
- Incident duration
- Incident timeline
  - Actions
  - Decisions
  - Information collected
- and etc.

**WHERE**
- Where is the attacks originated from?
- Attack paths
- Lateral movement
- Logical
  - Network zone
- Physical
  - Cloud
  - On-premises
- and etc.
Incident Reporting Basics (3)

**HOW**
- How does it happened?
- How the systems infected?
- What vulnerabilities exploited?
- Attack method
- Intrusion method
- Command and control
- Evade detection
- Obfuscation
- and etc.

**WHY**
- Why does it happened?
- Root cause
- and etc.
GDPR: British Airways faces record £183m fine for customer data breach

Information Commissioner’s Office intends to fine airline for “poor security arrangements” - British Airways says it’s “surprised and disappointed” by planned penalty.

By Danny Palmer | July 8, 2019 -- 07:50 GMT (15:50 GMT+08:00) | Topic: Security
Case Study | British Airways Data Breach Incident

- **What affected?**
  - Online booking website and the mobile app

- **What data had been stolen?**
  - Customer’s personal data (Names, billing address, email address)
  - Credit card or debit card details

- **How was it happened?**
  - Breaching by hiding JavaScript code known as Magecart
  - Customer booking data was sent to malicious site on submission

- **Why was it happened?**
  - Vulnerabilities being exploited that cause JavaScript injection on Modernizr module
185,000 transactions are compromised between April and July 2018

224,000 transactions are compromised between July and September 2018

23rd June
First detection

6th September
BA discloses the breach

Incident Response Process

Time:
- Apr 2018
- May 2018
- Jun 2018
- Jul 2018
- Aug 2018
- Sep 2018
Security Advice
Round Up
Being HACKED!? What to do next???
If you have provided login credentials in suspicious website, please reset password and review the security settings in the related online service accounts.
If you have provided financial information, such as credit card number, and incur financial loss, please contact your bank immediately.
You should report to nearby police station if any financial loss is incurred.
If someone **spoofs** your **identity** to send email to your family, friends and business partners, you should **alert them by other trusted communication channels**.
Contact your **IT Department** immediately!

if you have one...
Not being hack . . .
just YET !!!
Cybersec Infohub

Sharing

Collaboration

Trust
Cybersec Infohub

Threat information and analysis
Alerts, news, vulnerabilities
Mitigation advisories
Situational awareness
Best practices and tips
Strategic analysis

Key participants
ISPs
Critical Infrastructure
Critical Internet Infrastructure
IT & Security Vendors
Researcher
Local CERTs

Methods of Exchange
Via the Platform
Industry Event
Tele-conference
Webinar
Working Group
Our Community

Distribution of Top Five Sectors

141 MEMBERS

431 REPRESENTATIVES

Our Community

Distribution of Top Five Sectors

141 MEMBERS

431 REPRESENTATIVES

Hot Discussion Topics

Top posts shared on Cybersecinfohub with good responses from members in August 2019:

- MAS Directive on Cyber Hygiene.
- New Vulnerabilities in Remote Desktop Service (RDS) Affecting Most Current Windows Versions.
- Mozilla Firefox: Mozilla Firefox 72.0.1 ESR, 72.0.2, and 72.0.3 ESR Security

Note: The above posts are accessible to members only.

Active Contributors

Our applause to the following representatives for their active contributions to Cybersecinfohub in August 2019:

Ban CHENG
Sangfor Technologies (Hong Kong) Limited

Chester LAU
Palo Alto Networks

Claudius LAM
Trend Micro

Harry POON
SmarTone Mobile Communications Limited

Nick NG
Fortinet International, Inc.

Peony CHIU
Lapcon Limited

Cybersec Infohub Newsletter

August 2019 / Page 1
Hot Discussion Topics

Top posts shared on Cybersechub.hk with good responses from members in August 2019:

- iPhone Alert: Apple Accidentally Introduced A Critical Security Vulnerability In New iOS 12.4
- MAS Directive on Cyber Hygiene
- New Vulnerabilities in Remote Desktop Service (RDS) Affecting Most Current Windows Versions
- Shade 勒索軟件進一步活躍
- The Threat of BlueKeep (CVE-2019-0708) Becomes Imminent
- 全能挖礦病毒 GroksterMiner 來襲

Note: The above posts are accessible to members only.
Tips

Change your password regularly

As a security best practice, user passwords for the Members Zone are configured to expire in every 180 days.

You can change your password anytime via the “Change Password” function at “Settings”.

Want to share your professional advice to the public?

Create a TLP:WHITE post under “Advisories” or “Insights”, then click “Publish”.

Post will appear in the Public Zone upon confirmation by the Service Desk.

Want to create a group for close-group discussion?

From menu “Group”, click “Create Group Request”. Fill in the required information and send the request to the Service Desk.

Communication within a Group is accessible to the Group members only.
Events

Our first Cybersec Infohub Webinar – “ Threat Intelligence and Exchange from Past to Future” on 16 August 2019

On 16 August 2019, the first Cybersec Infohub webinar was held successfully, as a new channel to shore up our collaborative network. Thank you all the participants for joining the webinar, and we hope it was a fruitful one for everybody.

Can’t wait for the next webinar? Stay tuned!

If you have missed the valuable sharing, you may find the presentation slides, video recording and follow-up discussions in the Members Zone. (https://www.cybersechub.hk/platform/threat/620?nav=informationSharing:General%20Discussion)
Cybersec Infohub

cybersechub.hk
1. Everyone can be targeted, even you are just a small potato in your organization!

2. Set a strong password & enable 2FA whenever possible

3. Make sure your software / App are up-to-date & only download from reliable sources

4. Do the SAME to your home PC/laptop/mobile devices

5. Build your own Human Firewall
Question?
Thank You 🤗