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

- Latest Cyber Security Threats & Trends
- Cyber Attack & Defense
- Security Incidents Handling
- Security Advice Round Up
About Us

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

Website: www.hkcert.org
24-hour Hotline: 8105 6060
Email: hkcert@hkcert.org
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

Referred case contributed 95%

YoY ↑ 55%
Summary of HKCERT Security Incident Reports

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

Total ⇋ 55%

Source: HKCERT
Cyber Attack & Defense
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 legitimate website.
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>Percentage</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Email</td>
<td>77%</td>
<td>(+28%)</td>
</tr>
<tr>
<td>Ransomware</td>
<td>42%</td>
<td>(-10%)</td>
</tr>
<tr>
<td>Other Malware Attack including Botnet</td>
<td>22%</td>
<td>(-3%)</td>
</tr>
<tr>
<td>CEO Scam</td>
<td>18%</td>
<td>(-17%)</td>
</tr>
<tr>
<td>DDoS</td>
<td>14%</td>
<td>(+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)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Affected Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>47%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>42%</td>
</tr>
<tr>
<td>Retail</td>
<td>32%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>21%</td>
</tr>
</tbody>
</table>

- 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

- Use of HTTPS

  - 2015 Q1: 58% of phishing using HTTPS
  - 2019 Q1: 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 RAVI LAHSMANAN — 9 days ago in SECURITY
How To Distinguish PHISHING SCAM
TOP 10 GENERAL EMAIL SUBJECTS

1. Password Check Required Immediately
2. Your Order with Amazon.com/Your Amazon Order Receipt
3. Announcement: Change in Holiday Schedule
4. Happy Holidays! Have a drink on us.
5. Problem with the Bank Account
6. De-activation of [[email]] in Process
7. Wire Department
8. Revised Vacation & Sick Time Policy
9. Last reminder: please respond immediately
10. UPS Label Delivery 1ZBE312TNY00015011

Source: https://www.securitybrigade.com
GREED
CURIOUSITY
URGENCY
FEAR
How to distinguish Phishing Scams?

Sample 1
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

 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**

- **GENERAL GREETING**
  - 親愛的客戶，您好：

- **URGENCY**
  - 由於您MMA金融交易網的「使用者代碼」與「網路密碼」已逾八個月未變更，為確保您的網路交易安全，建議您不長期變更，謝謝！若您忘記使用者代碼或網路密碼，或登入錯誤多次導致無法使用，請您進入永豐網路銀行

**Retail**

- **GENERAL GREETING**
  - Dear iTunes Customer!

- **URGENCY**
  - Your iTunes account has been frozen because we are unable to validate your account information.
  - Once you have updated your account records, we will try again to validate your information.
  - Your account suspension will be lifted. This will help protect your account in the future.
  - This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

- **Get Started**
  - If you need help logging in, go to our Help line by clicking the Help link located in the upper right-hand corner of any Apple page.

  Sincerely,

  Apple Inc
How to distinguish Phishing Scams?

Sample 4

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

Sample 5

Enter the URL on your own
How to distinguish Phishing Scams?

Sample 6

Electronic Sports

INVALID DIGITAL CERTIFICATE

CURIOSITY

GREED
Protection against Phishing Attacks

1. Think before you click
2. Pick up the phone to verify
3. Use two-factor authentication (2FA) across all accounts
4. Use different passwords for different services
5. Use email filtering technology & make sure the technique is up-to-dated
6. Conduct phishing drill exercises for all general staff
Over **500 US schools** were hit by ransomware in 2019

Fifteen US school districts, accounting for **100 schools**, were hit in the **past two weeks alone**.

By Catalin Cimpanu for Zero Day

October 1, 2019 -- 14:24 GMT

(22:24 GMT+08:00) | Topic: Security
East Texas Attack

Port Neches-Groves schools paid an undisclosed amount via bitcoin to a suspected overseas cyberattacker who encrypted millions of the district's files and issued a four-day deadline to respond to the criminal demands.

By Isaac Winde, Beaumont Enterprise | November 20, 2019
Shade Ransomware Is the Most Actively Distributed Malware via Email

By Sergiu Gatlan

The graph shows the distribution of malware concealed in emails from 2017 to 2019. The categories include Ransomware, Loaders, Banking Trojans, Backdoors and remote access tools, Unwanted software, and Cryptomining malware.

- **2017**:
  - Ransomware: 40%
  - Loaders: 32%
  - Banking Trojans: 13%
  - Backdoors and remote access tools: 11%
  - Unwanted software: 2%
  - Cryptomining malware: 2%

- **2018**:
  - Ransomware: 24%
  - Loaders: 33%
  - Banking Trojans: 22%
  - Backdoors and remote access tools: 4%
  - Unwanted software: 3%
  - Cryptomining malware: 1%

- **2019**:
  - Ransomware: 14%
  - Loaders: 22%
  - Banking Trojans: 16%
  - Backdoors and remote access tools: 4%
  - Unwanted software: 3%
  - Cryptomining malware: 54%
MALSPAM-BASED SHADE RANSOMWARE INFECTION:

MALSPAM → LINK TO ARCHIVE, ATTACHED ARCHIVE, OR ATTACHED PDF WITH LINK TO ARCHIVE → JS OR OTHER SCRIPT-BASED FILE → COMPROMISED WEB SERVER → SHADE RANSOMWARE

Source: https://unit42.paloaltonetworks.com/shade-ransomware-hits-high-tech-wholesale-education-sectors-in-u-s-japan-india-thailand-canada/
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

Pay ransom on time or your DATA is PUBLICIZED

Pay ransom or INFECT 2 friends to get DATA back

Jigsaw
Doxware
Popcorn time
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
Experts: Don't reboot your computer after you've been infected with ransomware

Rebooting may lead to restarting a crashed file-encryption process, potential loss of encryption keys stored in-memory.

Source: https://www.zdnet.com/article/experts-dont-reboot-your-computer-after-youve-been-infected-with-ransomware/
Security Incidents
Handling
5WH1H

5 Why

1. What
2. Who
3. Why
4. When
5. How

IR

WHERE

WHY

WHO

WHAT
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.
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
Case Study | British Airways Data Breach Incident

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
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 !!!

Image credit: http://www.damazine.com/fishing-a-good-way-of-relaxing/
Cybersec Infohub

Sharing

Trust

Collaboration
Cybersec Infohub

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

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

Methods of Exchange
Via the Platform
Industry Event
Tele-conference
Webinar
Working Group
Cybersechub.hk | Members Zone

- Traffic Light Protocol
- User Anonymity
- Export IOCs for Operation
- Social Media “Like” Feature
- “KOL” of Cybersechub.hk
- Trusted Groups Discussion
- Private Messaging
- Directory for Connections
Our Community

141 Members
431 Representatives

Distribution of Top Five Sectors

Hot Discussion Topics
Top posts shared on CybersecHub.hk with good responses from members in August 2019:
- MAS Directive on Cyber Hygiene
- [New Vulnerabilities In Remote Desktop Service (RDS)] Affecting Most Current Windows Version
- [Onagiri] - The Threat of BlueKeep (CVE-2020-0601) Becomes Inevitable
- [From the BlackHole] - Looking at Cybersecurity + More

Note: The above posts are accessible to members only.

Active Contributors
Our applause to the following representatives for their active contributions to CybersecHub.hk in August 2019:

Ban CHENG - Saugier Technologies (Hong Kong) Limited
Chester LAU - Palo Alto Networks
Claudine LAM - Trend Micro
Harry POON - SmartTime Mobile Communications Limited
Nick NG - Fortinet International, Inc.
Penny CHUI - Lapesa Limited
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)
Bring these messages back to your school......

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 😊
Canon DSLR Camera Infected with Ransomware Over the Air
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?
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
Botnet (roBot Network)
Infrastructure of Controlled Victim Computers (BOTs)

Bot Herder

Up: Data
Down: Command/Update

C&C

bot

Spam, Malware & Phishing

victim

DDoS Attack