



網絡安全及科技罪案調查科

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU

Latest Cyber Security Situation in Medical Sector and in Hong Kong

*Ken Lee
Senior Inspector of Police
Collaboration Team 3, Cyber Security Division
Cyber Security and Technology Crime Bureau*

Cyber Attack Trend

Motives and Targets

- Government Bodies
- Large Corporations

- Critical Infrastructures
- Mobile Devices
- Internet of Things
- Smart City
- Cloud
- E-Payment
- Etc.....

- Individuals
- SMEs

- Advanced Persistent Threat
- Ransomware

- Malware
- DDoS Attack
- Hacking

- Defacement
- Virus



© HONG KONG POLICE FORCE 香港警務處版權所有

Case Sharing



Case Sharing

🏠 > News Highlights

SINGHEALTH'S IT SYSTEM TARGET OF CYBERATTACK

📅 20TH JUL 2018

JOINT PRESS RELEASE BY MCI AND MOH

SINGHEALTH'S IT SYSTEM TARGET OF CYBERATTACK

Safeguard Measures Taken, No Further Exfiltration Detected

SingHealth's database containing patient personal particulars and outpatient dispensed medicines has been the target of a major cyberattack.

2 About 1.5 million patients who visited SingHealth's specialist outpatient clinics and polyclinics from 1 May 2015 to 4 July 2018 have had their non-medical personal particulars illegally accessed and copied. The data taken include name, NRIC number, address, gender, race and date of birth. Information on the outpatient dispensed medicines of about 160,000 of these patients was also exfiltrated. The records were not tampered with, i.e. no records were amended or deleted. No other patient records, such as diagnosis, test results or doctors' notes, were breached. We have not found evidence of a similar breach in the other public healthcare IT systems.



SingHealth

Defining Tomorrow's Medicine



© HONG KONG POLICE FORCE 香港警務處版權所有

網絡安全及科技罪案調查科

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU

What do hackers do with your data?



Our Internet



HONG KONG POLICE FORCE 香港警務處版權所有

Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



© HONG KONG POLICE FORCE 香港警務處版權所有

Phishing Email

From: "Bank of America" customerservice@bankofamerican.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Bank of America 

Dear Customer,


At Bank of America, your satisfaction is our number one priority. We offer an Advanced Online Security option for our customers with our website and add Advanced Online Security to your account with your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will be required to visit your local branch to verify your information.

Thank you for helping us to make Bank of America the best.

If you are receiving this message and you are not enrolled in our online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department 

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Sincerely,
Paypal customer department

<http://66.160.154.156/catalog/paypal/>

Addresses do not match!



Phishing Website



Credit Card Misuse



© HONG KONG POLICE FORCE 香港警務處版權所有

網絡安全及科技罪案調查科

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU

Items purchased



© HONG KONG POLICE FORCE 香港警務處版權所有

Blackmail

It seems that, xxxxxxxxx, is your password. You may not know me and you are probably wondering

Subject:

It seems that, xxxxxxxxx, is your password. You may not know me and you are probably wondering

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, \$2900 is a fair price for our little secret. You can pay me via Bitcoin.

BTC Address: 1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
(It is cAsE sensitive, so copy and paste it)

警務處版權所有

Whatsapp Hijacking



© HONG KONG POLICE FORCE 香港警務處版權所有

How to login a Whatsapp?

We have sent you an SMS with a code to the number above.

To complete your phone number verification, please enter the 6-digit activation code.

Resend Code in 1:03

Call Me in 1:03



© HONG KONG POLICE FORCE 香港警務處版權所有

Two-step verification

The screenshot shows the WhatsApp account settings interface. On the left, a menu lists: Privacy, Security, Two-step verification, Change number, and Delete my account. The 'Two-step verification' option is selected. The main content area features a green padlock icon and the text: "For added security, enable two-step verification to require a passcode when registering your phone number with WhatsApp." Below this is a green "ENABLE" button. On the right, a text prompt asks to "Enter a six-digit passcode which you'll be asked for when you register your phone number with WhatsApp:" followed by a six-digit input field. Below the input field is a "NEXT" button and a numeric keypad with a green checkmark button.



Ransomware

Ransomware is a serious security threat that limits victims to access their files or system functions. It has “data-kidnapping” capabilities.

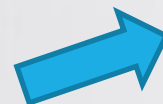
Cybercriminals tend to threaten victims to pay ransom (bitcoin) in order to regain access to their files or systems.



Ransomware



Email with
malicious
attachment



Open the email and
execute the
attachment



Bitcoin blackmail



© HONG KONG POLICE FORCE 香港警務處版權所有

Mitigation

- Unplug the power
- Disconnect the infected terminal from network
- Remove external storage devices from infected terminal
- Retain sample for analysis



Preventive Measures

Regular Backup

- Offsite backup
- Online backup



© HONG KONG POLICE FORCE 香港警務處版權所有

Preventive Measures

Management Solution

- Access Control
- Device Management
- Awareness of Staff
- Incident Response Mechanism
- Regularly update the OS
- Constantly review the security network



Current approach



Commissioner's Operational Priorities 2012 - 2018

COMMISSIONER'S OPERATIONAL PRIORITIES 2017

The Commissioner's Operational Priorities 2017 set out the key operational areas which the Force will accord priority to during the year. They are a continuation of the seven priorities identified last year with minor refinements to reflect our current operating environment and key challenges in the year ahead.

The successful implementation of these priorities will ensure that Hong Kong remains a safe and stable society.



COMMISSIONER'S OPERATIONAL PRIORITIES 2018

The Commissioner's Operational Priorities 2018 set out the key operational areas which the Force will accord priority to during the year. They are a continuation of the seven priorities identified last year with minor refinements to reflect our current operating environment and key challenges in the year ahead.

The successful implementation of these priorities will ensure that Hong Kong remains a safe and stable society.

HONG KONG POLICE FORCE

香港警務處版權所有

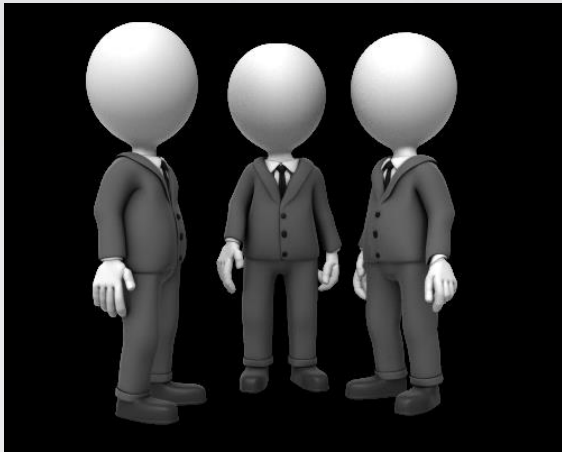
Current approach

Priorities

CYBER SECURITY AND TECHNOLOGY CRIME

- Promote public awareness of computer and cyber security as well as the risks associated with the Internet and social media through a multi-agency approach.
- Enhance cooperation with other law enforcement agencies to target technology crime.
- Strengthen coordination and sharing of expertise in handling and investigating technology crime.

Strategies



© HONG KONG POLICE FORCE 香港警務處版權所有

Prevention and Engagement Strategies



Instagram



© HONG KONG POLICE FORCE 香港警務處版權所有

Public Awareness

Cyber Security Seminars



Cyber Security Competition



© HONG KONG POLICE FORCE 香港警務處版權所有

Public Awareness

- **Cyber Security Professionals Awards**
 - Held in Feb 2018
 - Encourage the sharing of best practice in cyber security among Critical Infrastructures



© HONG KONG POLICE FORCE 香港警務處版權所有

Public Awareness

- **Cyber Security Consortium 2018**

- Held between 23 and 25 Oct 2018 (3 days)
- Attracted more than 600 law-enforcement officers, IT experts and industry leaders to attend



Public Awareness

- Cyber Security Campaign
 - <https://www.cybersecuritycampaign.com.hk/>
 - 1st Wave (Jun 2017) : Anti Botnet
 - 2nd Wave (Aug 2018) : Security of Smart Devices



警務處版權所有

“No More Ransom” Project

(www.nomoreransom.org)

Winner
EDITOR'S CHOICE AWARD

NO MORE RANSOM!

★ English

Crypto Sheriff Ransomware: Q&A Prevention Advice Decryption Tools Report a Crime Partners About the Project

< New decryptor for **LambdaLocker** available, please click [here](#). >

NEED HELP unlocking your digital life
without paying your attackers*?

YES NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

GOOD NEWS

GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a

Unfortunately, in many cases, once the ransomware has been released into your device

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted

HKPF has joined the anti-ransomware project “No More Ransom”, which was initiated by Europol, the Dutch National Police and two cyber security companies.

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU

網絡安全及科技罪案調查科

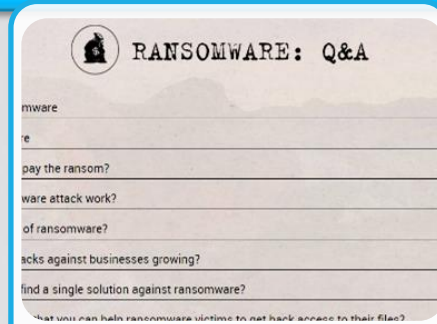
© Hong Kong Police Force 香港警務處版權所有

“No More Ransom” Project

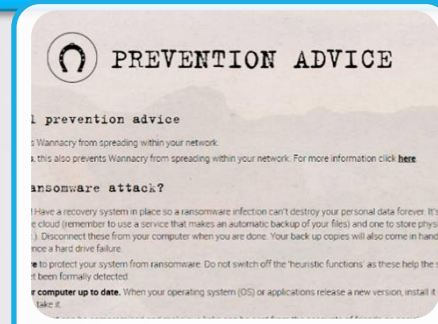
(www.nomoreransom.org)



Analysis of Ransomware



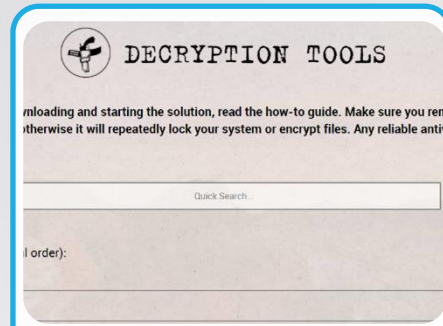
Online Database



Prevention Advice



www.nomoreransom.org



Decryption Tools



Reporting to Law Enforcement



https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/project_nmr.html

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU

網絡安全及科技罪案調查科

© Hong Kong Police Force 香港警務處版權所有

“No More Ransom” Project

(www.police.gov.hk)

香港特別行政區政府
香港警務處

GovHK 香港政府一站通 簡 | EN 文字版本 A- A A+

歡迎瀏覽香港警務處網頁

主頁 · 刑事事項 · 網絡安全及科技罪案

“拒絕勒索軟件”計劃

NO MORE RANSOM!

Crypto Sheriff Ransomware Q&A Prevention Advice Decryption Tools Report a Crime Partners About the Project

For more information on prevention advice for WannaCry, please click [here](#).

NEED HELP unlocking your digital life
without paying your attackers*?

YES **NO**

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS **BAD NEWS** **GOOD NEWS**

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a
Unfortunately, in many cases, once the ransomware has been released into your device
Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted

為加強國際間的多機構合作並積極打擊加密勒索軟件，香港警務處加入了一個由歐洲刑警組織、荷蘭警方及兩間網路安全公司展開的“拒絕勒索軟件(No More Ransom)”計劃。透過與不同執法機構和資訊科技界合作，這個全球性打擊加密勒索軟件計劃，設立了網上平台 (www.no

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU



Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems

— *Kevin Mitnick* —

AZ QUOTES



© HONG KONG POLICE FORCE 香港警務處版權所有

Thank You



© HONG KONG POLICE FORCE 香港警務處版權所有

網絡安全及科技罪案調查科

CYBER SECURITY AND TECHNOLOGY CRIME BUREAU