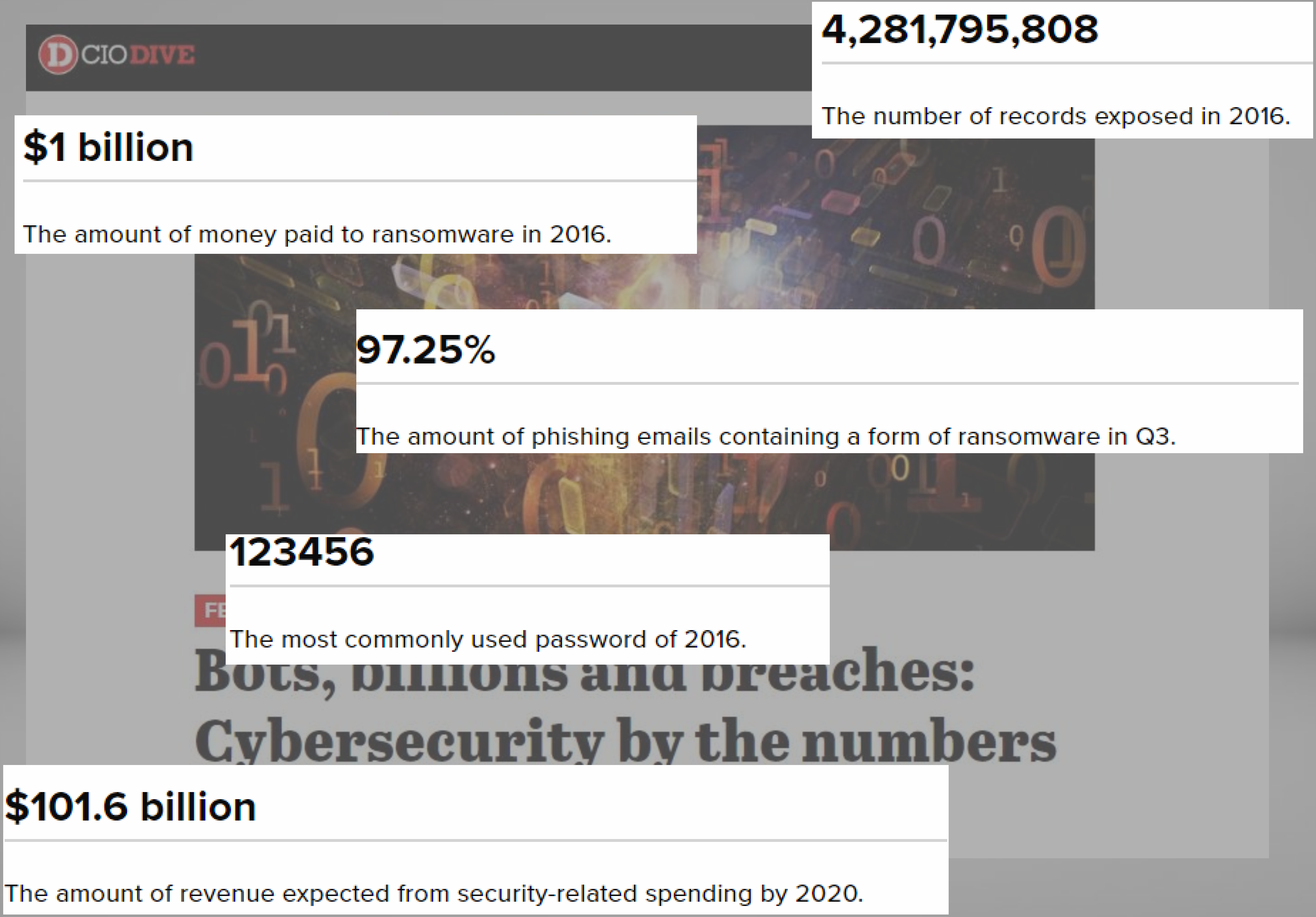
Cyber Security and Technology Crime Bureau

Dicky Wong

Senior Inspector of Police

Cyber Security Situation 2016 Review



CIO DIVE

4,281,795,808

The number of records exposed in 2016.

$1 billion

The amount of money paid to ransomware in 2016.

97.25%

The amount of phishing emails containing a form of ransomware in Q3.

123456

The most commonly used password of 2016.

FE

Bots, billions and breaches: Cybersecurity by the numbers

$101.6 billion

The amount of revenue expected from security-related spending by 2020.

Current approach

Hong Kong Police Force

COMMISSIONER'S OPERATIONAL PRIORITIES 20

The Commissioner's Operational Priorities 2012 set out the key operational areas that we must addre the year ahead.

There are seven priorities, each representing a significant challenge. This year, Technology Crime has b added and there are some refinements to ongoing priorities that bring them in line with changes in operational situation.

In addressing the Commissioner's Operational Priorities, it is important that we maintain public confide and support through our professionalism as we continue to serve with Pride and Care.

Hong Kong Police Force

COMMISSIONER'S OPERATIONAL PRIO

The Commissioner's Operational Priorities 2013 set out the key operational areas to wh priority during the year.

None of these seven priorities are new but refinements have been made to reflect operational environment and future challenges. This year, a sub-section on Major Inc been added to the area on Public Safety to address the need for greater preparedness of the changing environment and social developments.

The successful implementation of these priorities will ensure that Hong Kong remains a

Hong Kong Police Force

Hong Kong Police Force

missioner's Operational Priorities 2015

issioner's Operational Priorities 2015 set out the key operational areas to which the ccord priority during the year.

ain seven priorities this year but refinements have been made to reflect recent the operational environment and future challenges.

ful implementation of these priorities will ensure that Hong Kong remains a safe society.

Hong Kong Police Force

Commissioner's Operational Priorities 2016

The Commissioner's Operational Priorities 2016 set out the key operational areas to which the Force will accord priority during the year. They are a continuation of the seven priorities identified last year with minor refinements.

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

Hong Kong Police Force

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 2012 - 2017

Crime Trend

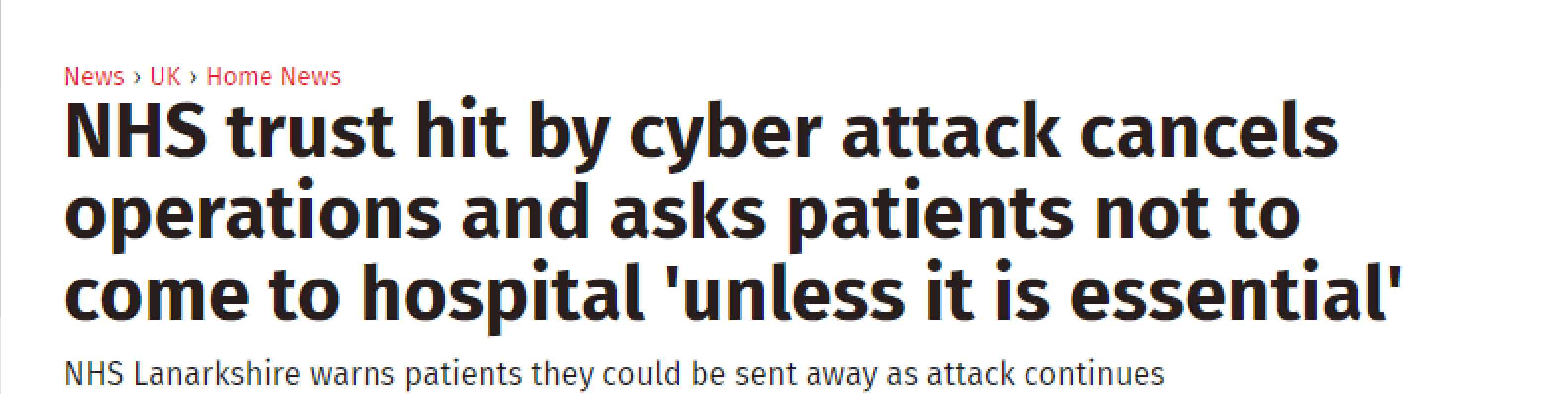
Year	Loss (Million)
2011	148.5
2012	340.4
2013	916.9
2014	1,200.6
2015	1,828.9
2016	2,300.8

Overall Crime

Technology Crime

(2017)	Loss (Million)
5567	1,393

Cyber Security Incidents



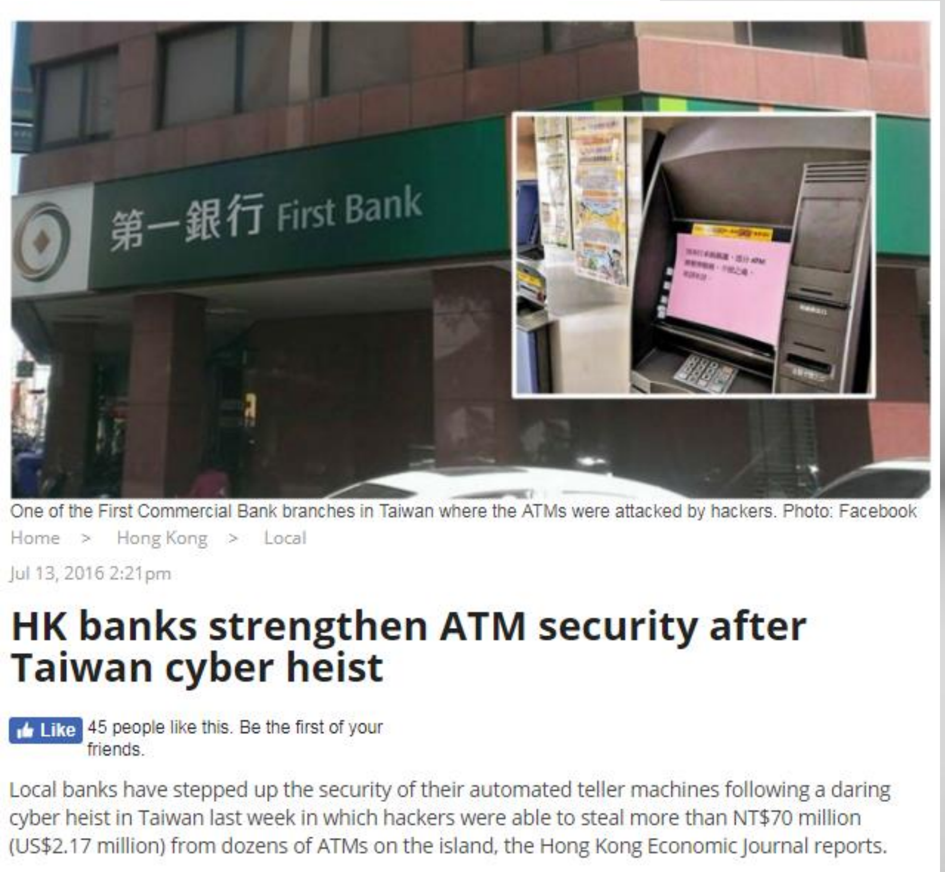
News › UK › Home News

NHS trust hit by cyber attack cancels operations and asks patients not to come to hospital 'unless it is essential'

NHS Lanarkshire warns patients they could be sent away as attack continues

Lizzie Dearden Home Affairs Correspondent | @lizziedearden | Saturday 26 Au

92 shares



One of the First Commercial Bank branches in Taiwan where the ATMs were attacked by hackers. Photo: Facebook

Home > Hong Kong > Local

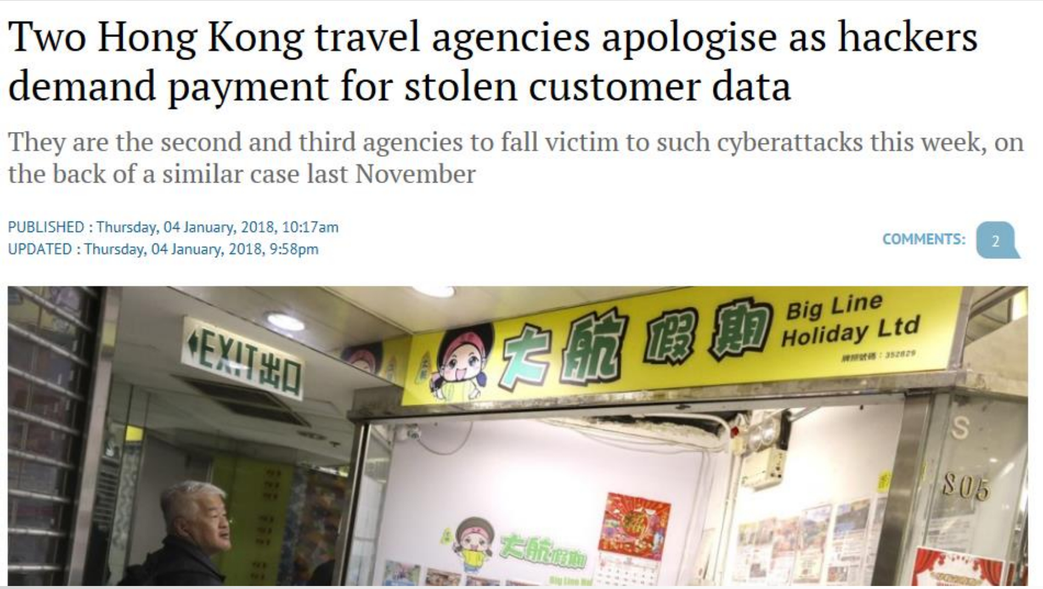
Jul 13, 2016 2:21pm

HK banks strengthen ATM security after Taiwan cyber heist

Like 45 people like this. Be the first of your friends.

Local banks have stepped up the security of their automated teller machines following a daring cyber heist in Taiwan last week in which hackers were able to steal more than NT$70 million (US$2.17 million) from dozens of ATMs on the island, the Hong Kong Economic Journal reports.

Cyber Security Incidents

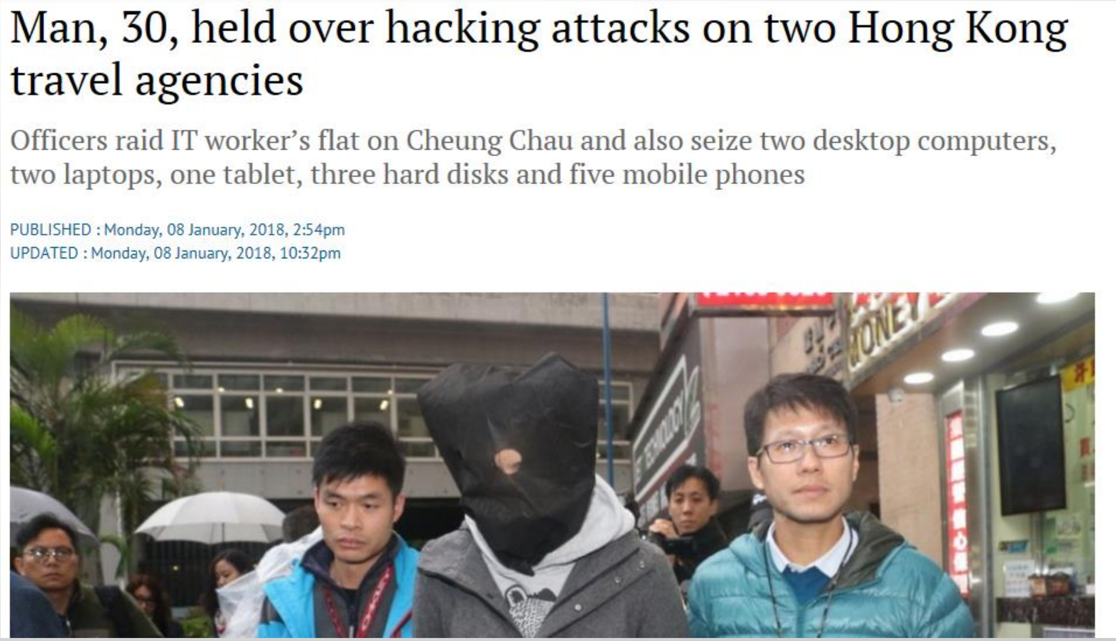


Two Hong Kong travel agencies apologise as hackers demand payment for stolen customer data

They are the second and third agencies to fall victim to such cyberattacks this week, on the back of a similar case last November

PUBLISHED : Thursday, 04 January, 2018, 10:17am
UPDATED : Thursday, 04 January, 2018, 9:58pm

COMMENTS: 2



Man, 30, held over hacking attacks on two Hong Kong travel agencies

Officers raid IT worker’s flat on Cheung Chau and also seize two desktop computers, two laptops, one tablet, three hard disks and five mobile phones

PUBLISHED : Monday, 08 January, 2018, 2:54pm
UPDATED : Monday, 08 January, 2018, 10:32pm

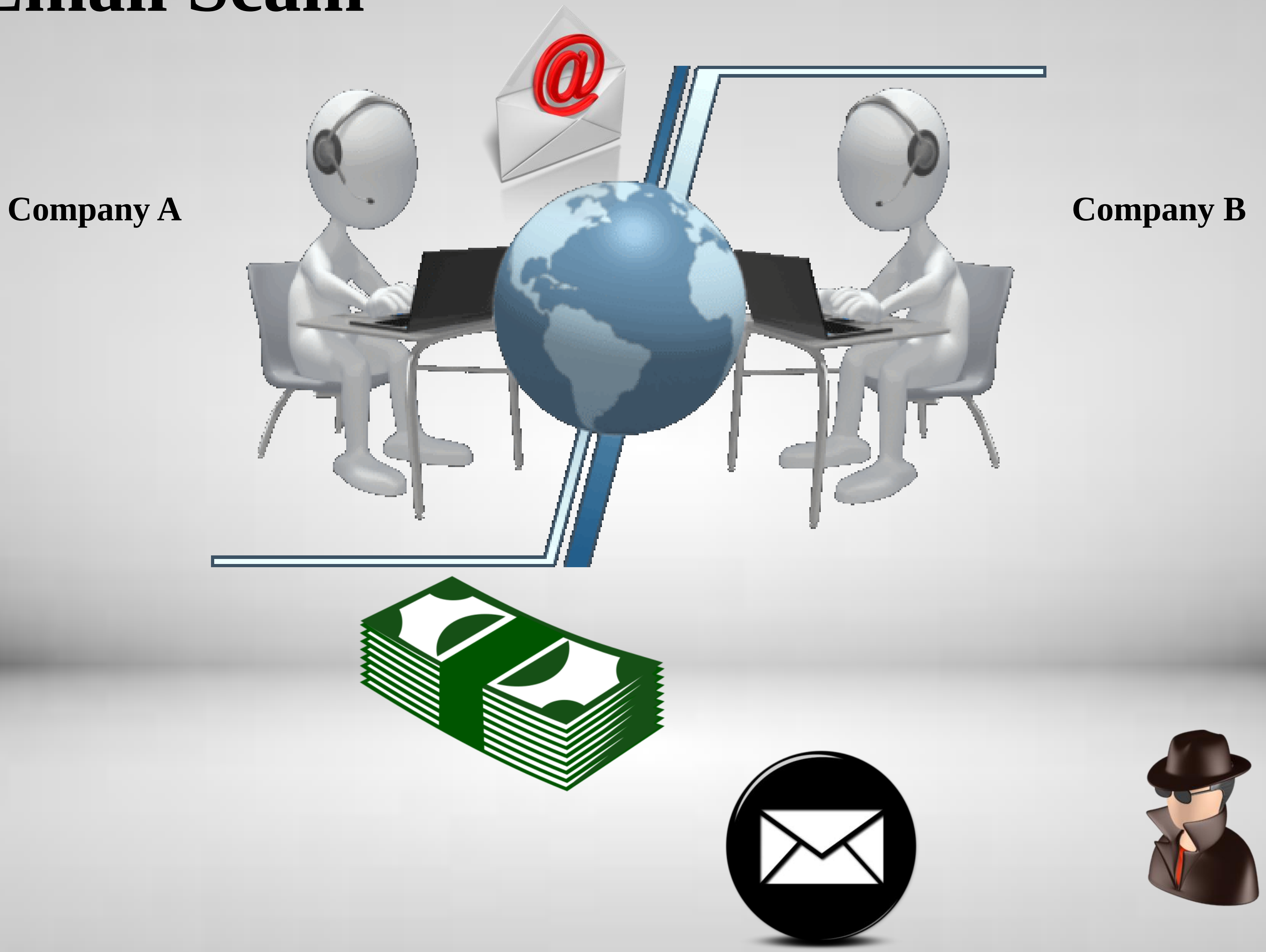
Cyber Threats

Common types of Cyber Attack

"Trusted Source"
Information Update Required
Personal Information
Credit Card Information
Bank Account Information
Username
Old Password
New Password
Title
Please Select
First Name
Last Name
Gender
Male ○
Female ○
Birthday
Social Security Number
Company
Address 1
Address 3
City / Town
County
State / Province
ZIP / Postal Code
Country
United States
OK
Cancel

Phishing Email/ Website

Email Scam



Company A

Company B

CEO Email Scam

CEO Email Scam

騙款1000萬美

，較2

的3100萬急增至去年的2.21億。騙徒主要針

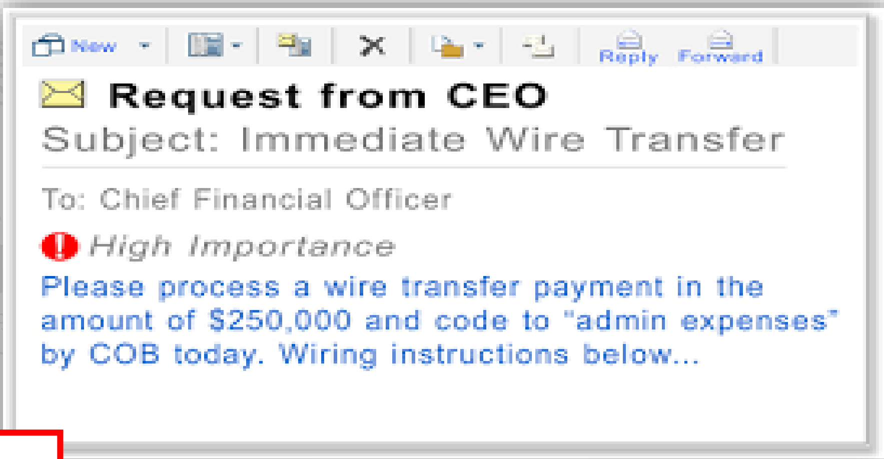
注意，待

司的首席財務官，要求匯款至客戶戶口。

CEO's email account was hacked

Hacker purported to be the CEO

Requested the CFO to make a fund transfer



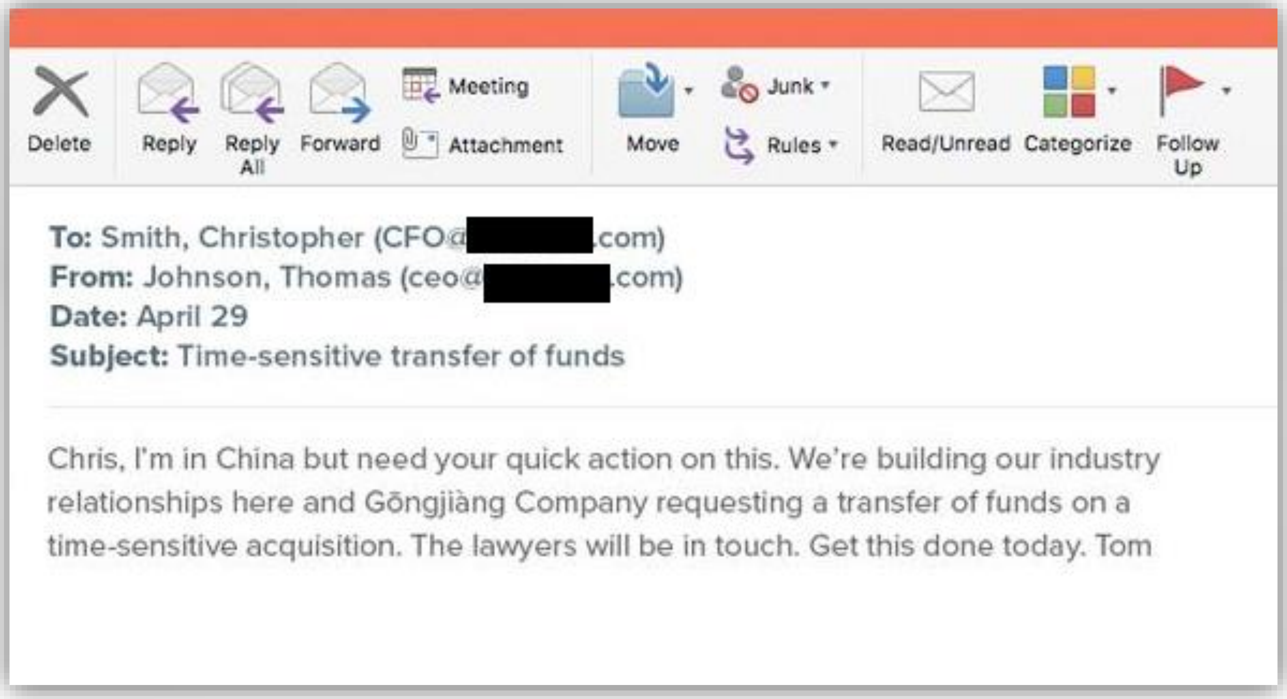
Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...



To: Smith, Christopher (CFO@[redacted].com)
From: Johnson, Thomas (ceo@[redacted].com)
Date: April 29
Subject: Time-sensitive transfer of funds

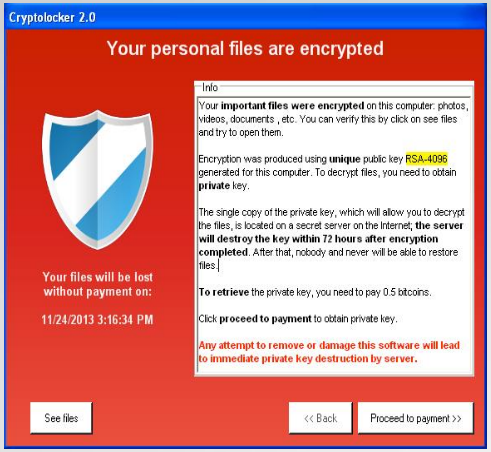
Chris, I'm in China but need your quick action on this. We're building our industry relationships here and Gōngjiàng Company requesting a transfer of funds on a time-sensitive acquisition. The lawyers will be in touch. Get this done today. Tom

Cyber Threats

Common types of Cyber Attack

Malware/ Ransomware

Ransomware



Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

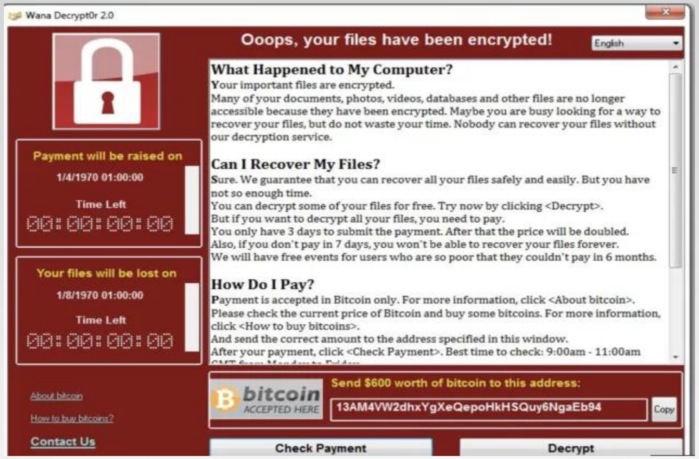
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

CryptoLocker



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

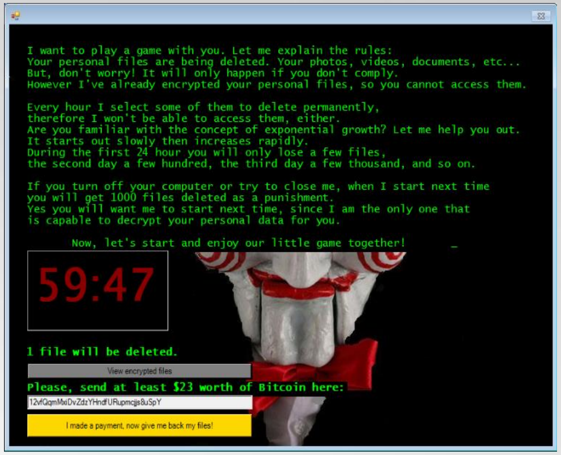
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

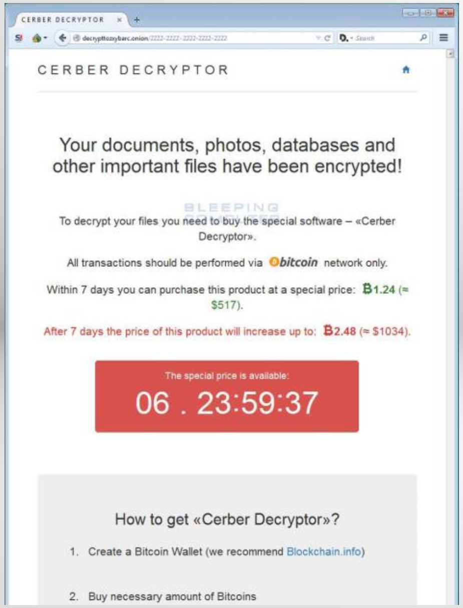
Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

WannaCry



```
I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hour you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted as a punishment.
Yes you will want me to start next time, since I am the only one that
is capable to decrypt your personal data for you.

      Now, let's start and enjoy our little game together!

59:47

1 file will be deleted.

Please, send at least $23 worth of Bitcoin here:
12vfQqmMxiDvZdzYHndfURupmcjjs8uSpY
```

Jigsaw



CERBER DECRYPTOR

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via bitcoin network only.

Within 7 days you can purchase this product at a special price: Ƀ1.24 (≈ $517).

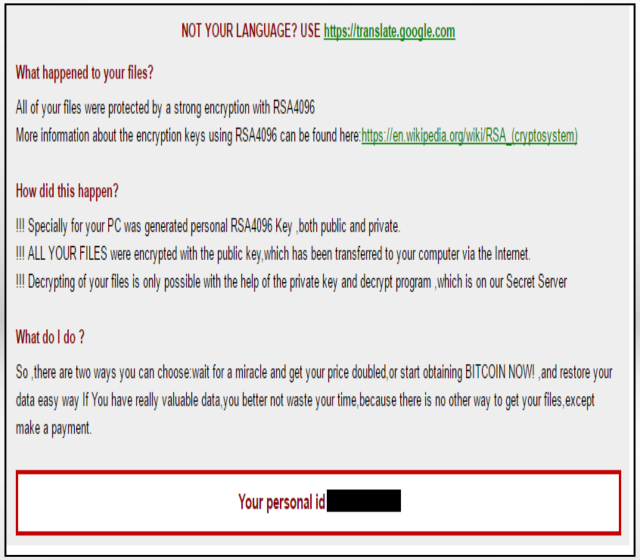
After 7 days the price of this product will increase up to: Ƀ2.48 (≈ $1034).

The special price is available:
06 . 23:59:37

How to get «Cerber Decryptor»?

1. Create a Bitcoin Wallet (we recommend Blockchain.info)
2. Buy necessary amount of Bitcoins

Cerber



NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files?

All of your files were protected by a strong encryption with RSA4096
More information about the encryption keys using RSA4096 can be found here:https://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen?

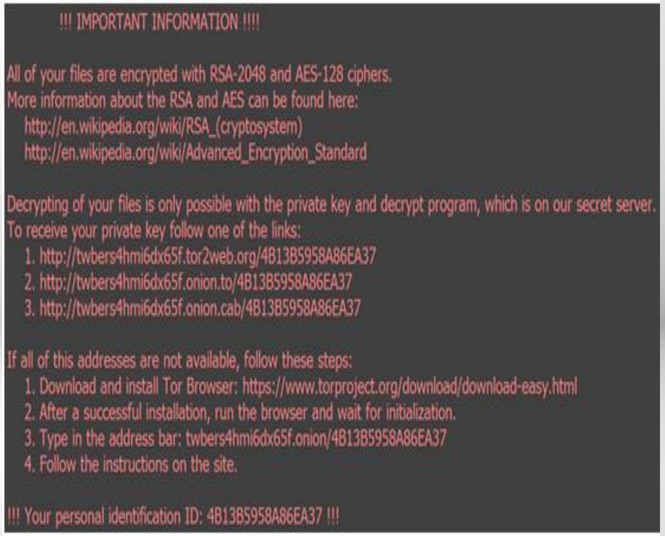
!!! Specially for your PC was generated personal RSA4096 Key ,both public and private.
!!! ALL YOUR FILES were encrypted with the public key,which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program ,which is on our Secret Server

What do I do ?

So ,there are two ways you can choose:wait for a miracle and get your price doubled,or start obtaining BITCOIN NOW! ,and restore your data easy way If You have really valuable data,you better not waste your time,because there is no other way to get your files,except make a payment.

Your personal id [redacted]

CryptXXX V3.0



!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. http://twbers4hmi6dx65f.tor2web.org/4B13B5958A86EA37
2. http://twbers4hmi6dx65f.onion.to/4B13B5958A86EA37
3. http://twbers4hmi6dx65f.onion.cab/4B13B5958A86EA37

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: twbers4hmi6dx65f.onion/4B13B5958A86EA37
4. Follow the instructions on the site.

!!! Your personal identification ID: 4B13B5958A86EA37 !!!

Locky

Preventive Measures

Preventive Measures

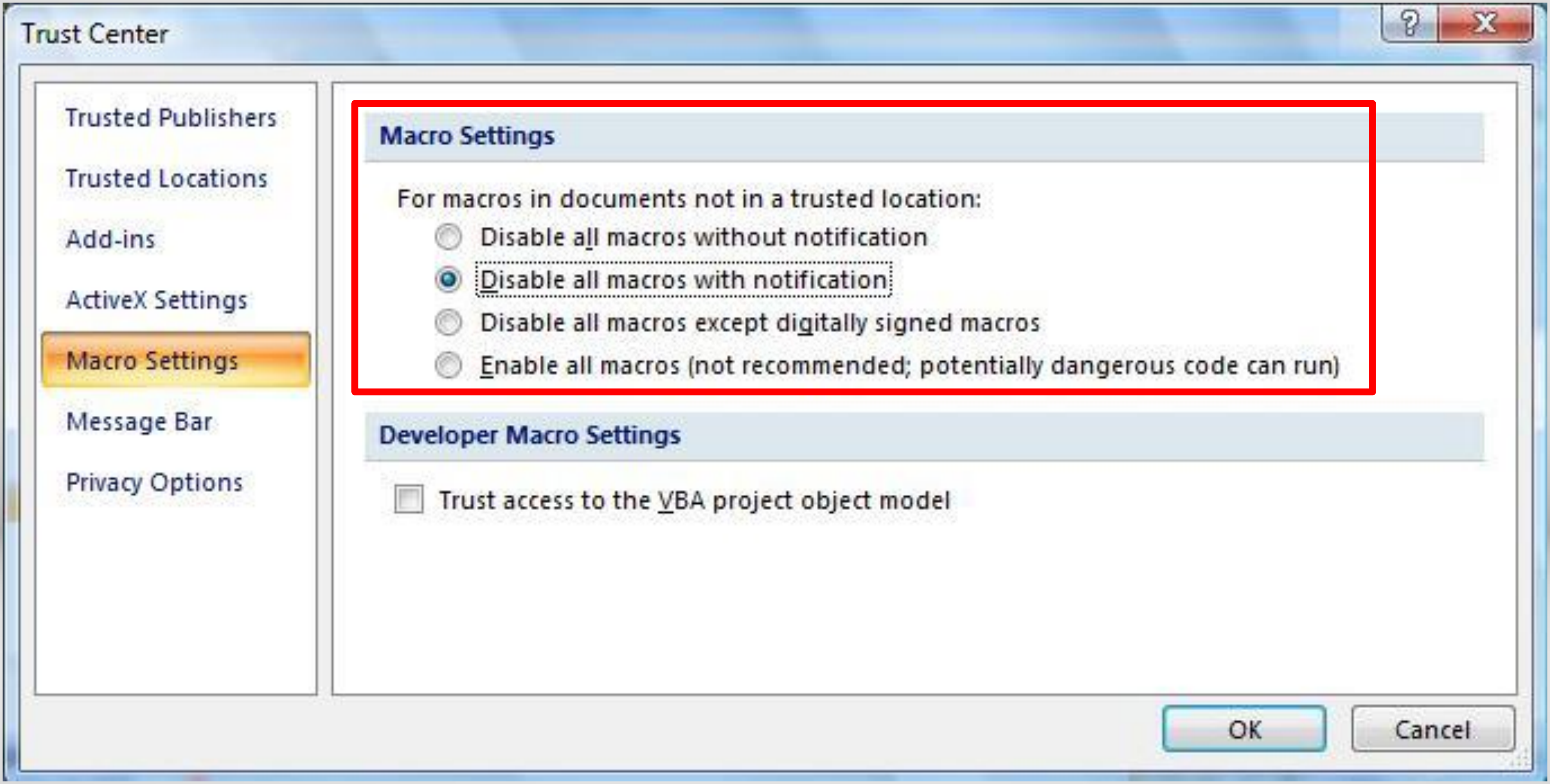
Suspicious Attachment

1. summary.exe, quotation.rar, payment.js

2. summary.doc, quotation.xlsx, statement.ppt

Preventive Measures

Disable Macros



Macro Settings

For macros in documents not in a trusted location:

○ Disable all macros without notification

● Disable all macros with notification

○ Disable all macros except digitally signed macros

○ Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

□ Trust access to the VBA project object model

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

Preventive Measures

Management Solution

- ➢Access Control
- ➢Device Management
- ➢Awareness of Staff
- ➢Incident Response Mechanism

Prevention and Engagement Strategies

- Anti-Botnet Operation
  - https://www.cybersecuritycampaign.com.hk/
  - Objective is to build a Botnet free city

CYBER SECURITY
CAMPAIGN
2017
BOT
BUILD A BOTNET-FREE CITY
Hong Kong Police Force
www.police.gov.hk
CSTCB
Cyber Security Campaign 2017
www.cybersecuritycampaign.com.hk
Supporting Organisation:
KASPERSKY lab
Symantec.
TREND MICRO 趨勢科技
珠海學院 CHU HAI COLLEGE OF HIGHER EDUCATION
港燈 HK Electric
HKT
PCCW
香港中文大學 The Chinese University of Hong Kong
PolyU
香港公開大學 THE OPEN UNIVERSITY OF HONG KONG
COMPUTER SCIENCE

Thank You