

Important Notice

All rights, including copyright, in this PowerPoint file are owned and reserved by the Hong Kong Police Force. Unless prior permission in writing is given by the Commissioner of Police, you may not use the materials other than for your personal learning and in the course of your official duty.

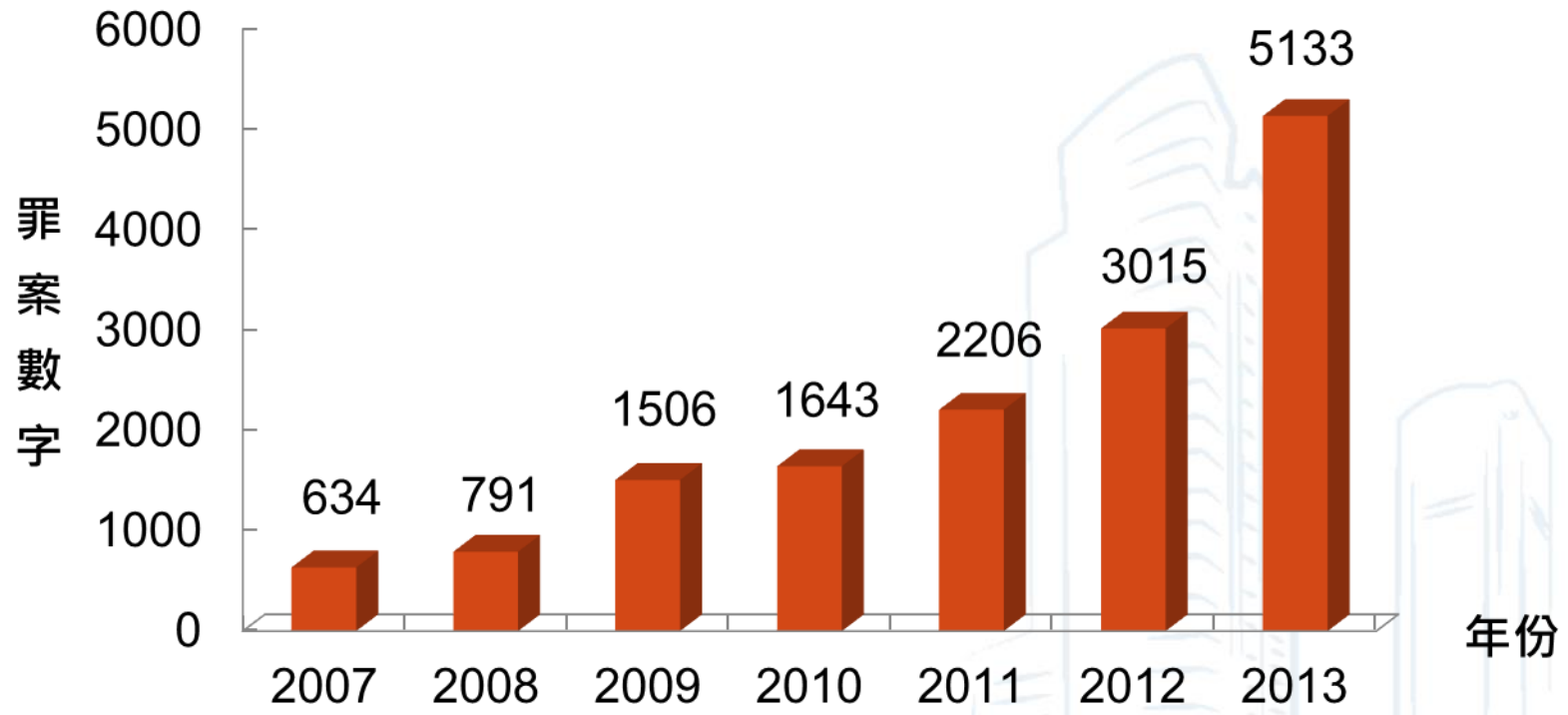
重要告示

香港警務處持有並保留本簡報檔案包括版權在內的所有權益。除預先獲得警務處處長書面許可外，本簡報檔案只可用作個人學習及處理公務上用途。

科技罪案數字



We serve with pride and care 服務為本精益求精



勒索軟件



We serve with pride and care 服務為本精益求精

CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
<http://feyrckkwjymeo.org/1002.exe>

Approximate destruction time of your private key:
2013-10-11 10:23

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique public key RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount in another currency**.

Click «Next» to select the method of payment and the currency.

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

Private key will be destroyed on
9/13/2013
5:27 AM

Time left
71 : 19 : 53

Next >>



【】國際黑客入侵本港學校收取「解毒費」，成為網上勒索新招。

早前收到一封懷疑偽冒學校的電郵，一名老師開啓後電腦即中毒「冧機」，螢光幕彈出訊息，要求事主透過虛擬貨幣Bitcoin繳付三百歐元（約三千二百港元）以解除病毒，否則將永遠不能開啓該電腦。由於學校伺服器亦中招癱瘓，校方遂報警求助。消息稱，案件犯案手法新穎罕見，恐成為新趨勢，初步相信為海外黑客「高手」所為，正追查電郵來源及黑客身份。

開啓後電腦中毒冧機



虛擬貨幣Bitcoin

位於，上周二（二十二日）有老師使用校內電腦時，錯誤開啓一封懷疑偽冒學校的電郵，老師不以為然，自行刪除作罷，翌日（二十三日）上班時，竟發現該電腦被鎖，屏幕全黑，疑遭病毒入侵，更彈出一則英文訊息，要求「中招者」繳付三百歐元Bitcoin，否則無法解除病毒。而學校的伺服器亦因病毒入侵而癱瘓，校方認為事態嚴重，遂於上周四（二十四日）下午一時許向警方報案。

無法解除病毒



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **29/03/14 - 09:10** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Your system: First connect IP: Total encrypted 4612 files.

[Refresh](#) [Payment](#) [FAQ](#) [My screen](#) [Test decrypt](#)

We are present a special software - CryptoDefense Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoDefense decrypter?

1. You should register Bitcoin wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com](#) - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
- [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Recommended for fast, simple service.
- [Coinbase](#) - Bitcoin exchange based in the United States. (Highly rated).
- [BitStamp](#) - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.

3. Send 0.9 BTC to Bitcoin address: 1EmLJ8peW292zRZVvumYPPa9wLcK4CPK1 [Get QR code](#)

4. Enter the Transaction ID and select amount:

Cryptodefense

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available [here](#).

Follow these simple steps if files recovery is needed:

1. Download and install Tor Browser.
2. Open Tor Browser and visit <http://cypheXfftr7hho.onion>. This link works **only** with the Tor Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is [\[redacted\]](#) (also visible [here](#)).
5. Follow the instructions on the [decryption page](#) once a valid decryption key has been acquired.

Technical details about the encryption process:

- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwritten with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.
- Once a valid decryption key is provided, the software search each files for a specific string stored in all encrypted files.
- When the string is found, the software extracts and decrypts the unique 256-bit AES key needed to restore that file.

Note: Without the decryption key, all encrypted files will be lost forever.

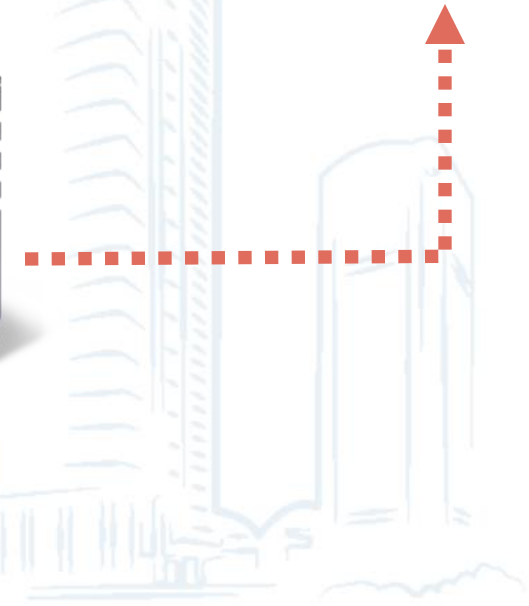
Copyright © 2014 SynoLocker™ All Rights Reserved.

SynoLocker

資料被盜取



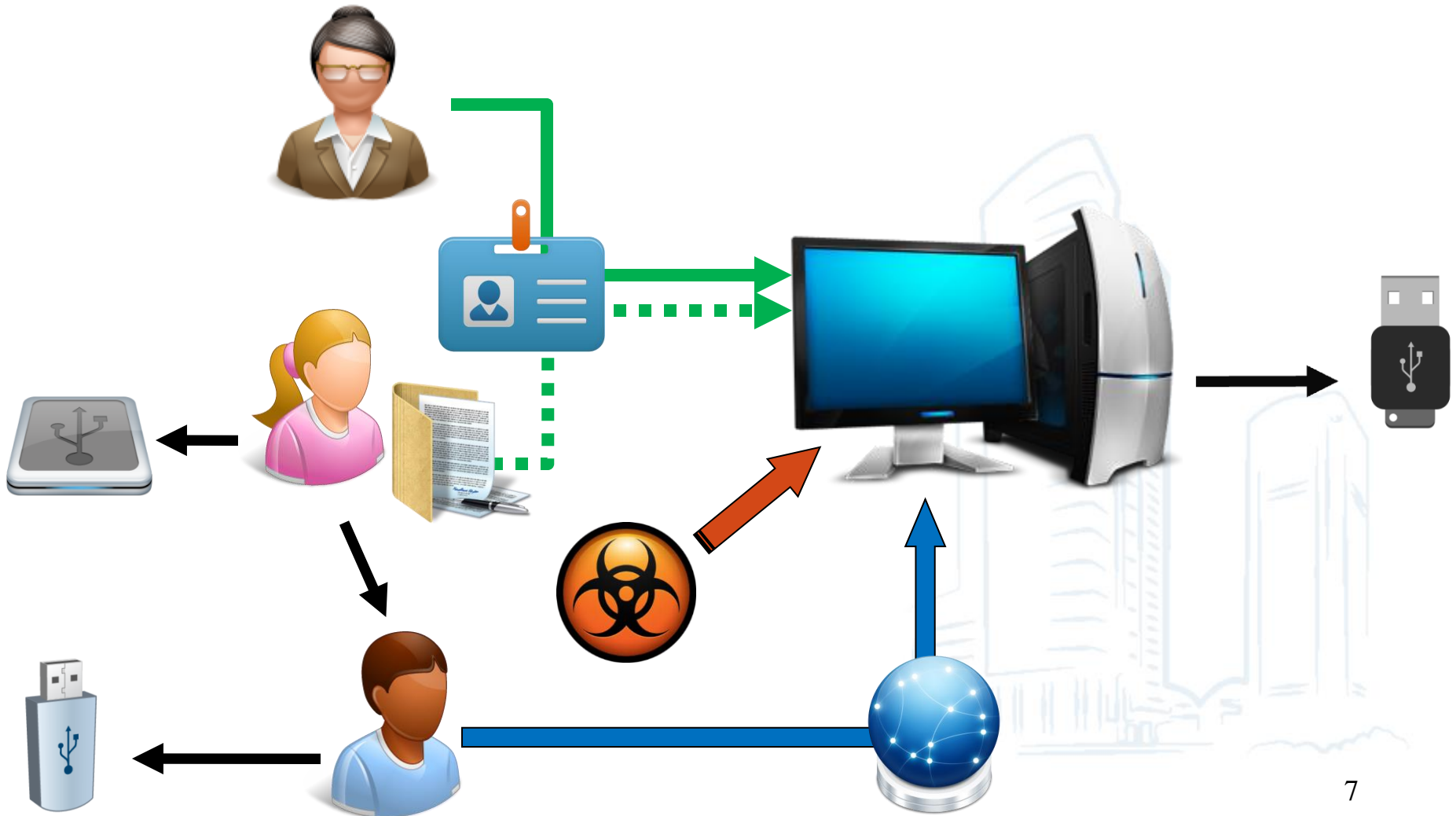
We serve with pride and care 服務為本精益求精



擅用他人戶口



We serve with pride and care 服務為本精益求精



預防方法



We serve with pride and care 服務為本精益求精

- 小心保管網上帳戶的資料 (登入名稱和密碼)
- 不要在互聯網上隨便透露個人資料 (例如地址、出生日期、身份證號碼、電話號碼、信用卡號碼或有關行程安排等資料)

預防方法



We serve with pride and care 服務為本精益求精

- 不要隨意開啟來歷不明的電郵及其附件
- 定期更改密碼
- 確定已開啟防火牆
- 定期更新修補程式
- 定期更新病毒及間諜軟體定義
- 用防毒軟體掃描電腦





We serve with pride and care 服務為本精益求精

Thank You