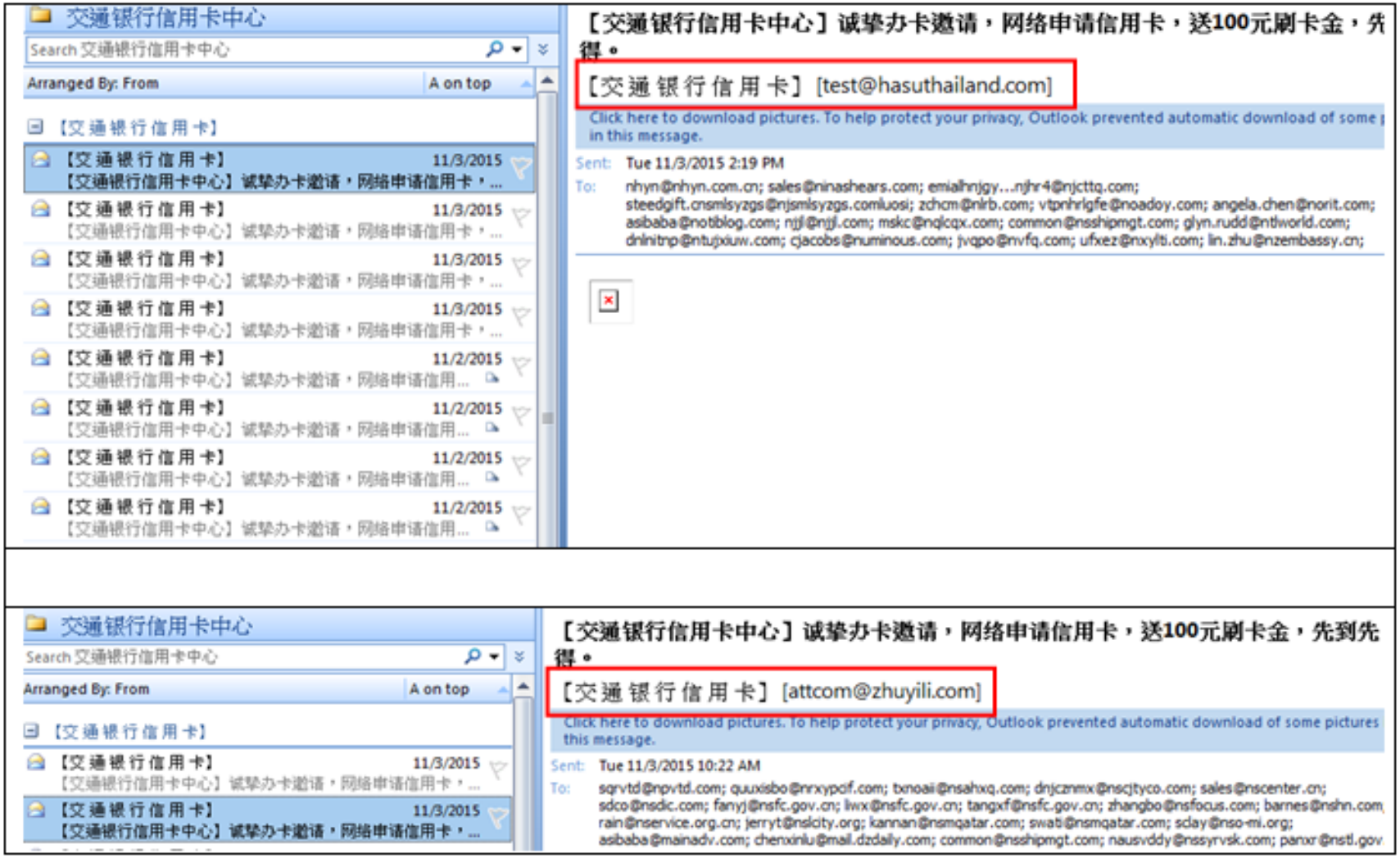
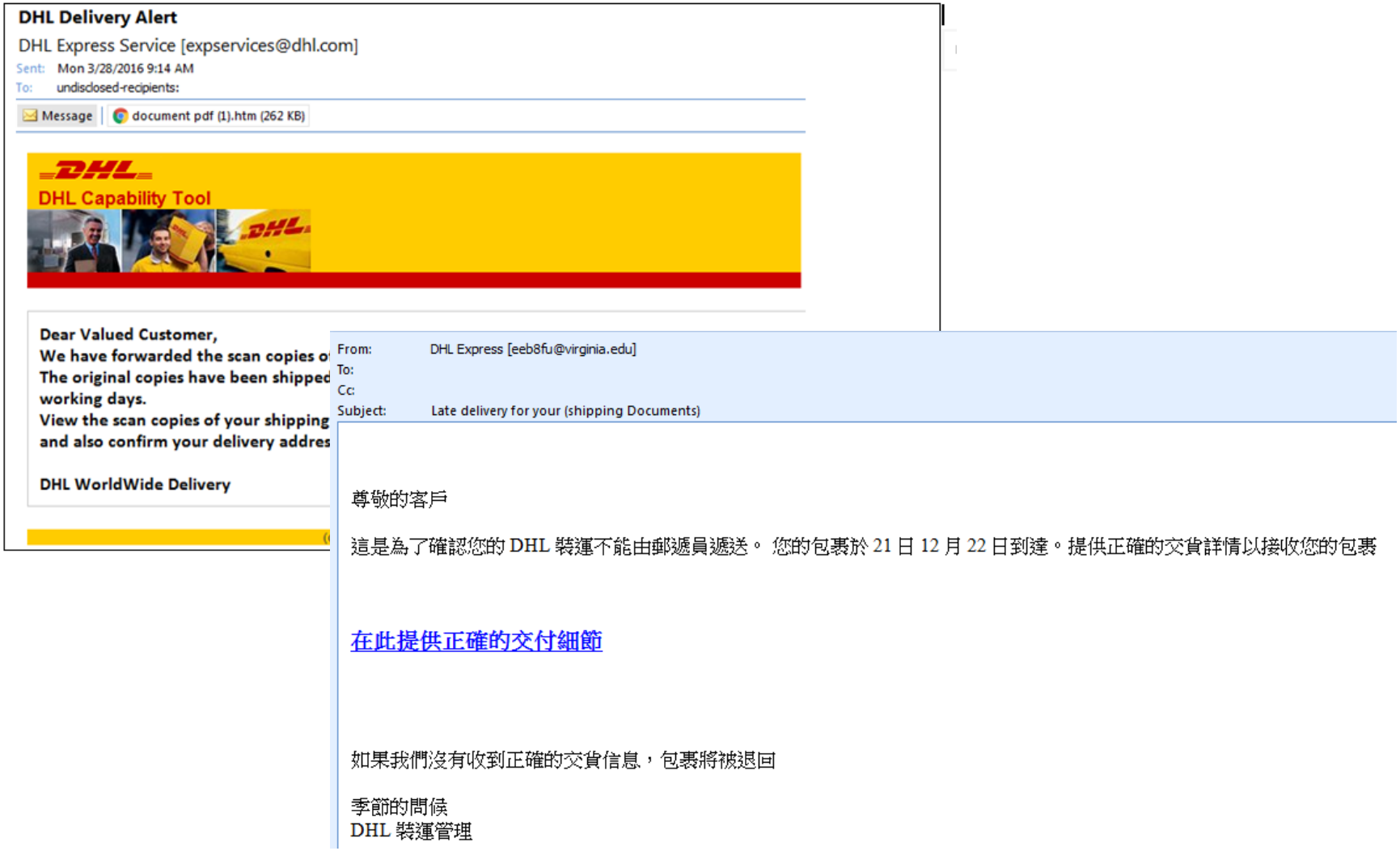
常見假冒郵件(銀行推廣)


交通银行信用卡中心
Search 交通银行信用卡中心
Arranged By: From
A on top
【交通银行信用卡】
【交通银行信用卡】 11/3/2015
【交通银行信用卡中心】诚挚办卡邀请，网络申请信用卡，...
【交通银行信用卡】 11/2/2015
【交通银行信用卡中心】诚挚办卡邀请，网络申请信用...
【交通银行信用卡中心】诚挚办卡邀请，网络申请信用卡，送100元刷卡金，先得。
【交通银行信用卡】[test@hasuthailand.com]
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
Sent: Tue 11/3/2015 2:19 PM
To: nhyn@nhyn.com.cn; sales@ninashears.com; emiallhnjgy...njhr4@njcttq.com; steedgift.cnsmlsyzgs@njsmlsyzgs.comluosi; zchcm@nlrb.com; vtpnhrlgfe@noadoy.com; angela.chen@norit.com; asibaba@notiblog.com; njjl@njjl.com; mskc@nqlcqx.com; common@nsshipmgt.com; glyn.rudd@ntlworld.com; dnlnitnp@ntujxiuw.com; cjacobs@numinous.com; jvqpo@nvfq.com; ufxez@nxylti.com; lin.zhu@nzembassy.cn;
交通银行信用卡中心
Search 交通银行信用卡中心
Arranged By: From
A on top
【交通银行信用卡】
【交通银行信用卡】 11/3/2015
【交通银行信用卡中心】诚挚办卡邀请，网络申请信用卡，...
【交通银行信用卡】 11/3/2015
【交通银行信用卡中心】诚挚办卡邀请，网络申请信用卡，...
【交通银行信用卡中心】诚挚办卡邀请，网络申请信用卡，送100元刷卡金，先到先得。
【交通银行信用卡】[attcom@zhuyili.com]
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures this message.
Sent: Tue 11/3/2015 10:22 AM
To: sqrvtd@npvtd.com; quuxisbo@nrxypcif.com; txnoaii@nsahxq.com; dnjcznmx@nscjtyco.com; sales@nscenter.cn; sdco@nsdic.com; fanyj@nsfc.gov.cn; liwx@nsfc.gov.cn; tangxf@nsfc.gov.cn; zhangbo@nsfocus.com; barnes@nshn.com; rain@nservice.org.cn; jerryt@nslcity.org; kannan@nsmqatar.com; swati@nsmqatar.com; sclay@nso-mi.org; asibaba@mainadv.com; chenxinlu@mail.dzdaily.com; common@nsshipmgt.com; nausvddy@nssyrvsk.com; panxr@nstl.gov

常見假冒郵件(DHL收件信)



DHL Delivery Alert

DHL Express Service [expservices@dhl.com]

Sent: Mon 3/28/2016 9:14 AM

To: undisclosed-recipients:

Message | document pdf (1).htm (262 KB)

DHL Capability Tool

Dear Valued Customer,
We have forwarded the scan copies o
The original copies have been shipped
working days.
View the scan copies of your shipping
and also confirm your delivery addres

DHL WorldWide Delivery

From: DHL Express [eeb8fu@virginia.edu]

To:

Cc:

Subject: Late delivery for your (shipping Documents)

尊敬的客戶

這是為了確認您的 DHL 裝運不能由郵遞員遞送。 您的包裹於 21 日 12 月 22 日到達。提供正確的交貨詳情以接收您的包裹

在此提供正確的交付細節

如果我們沒有收到正確的交貨信息，包裹將被退回

季節的問候
DHL 裝運管理

常見假冒郵件(附加病毒檔)

Message has a suspicious part : NEW ORDER (TO DURBAN)

mahmoued elbaz [hustara@gmail.com]

Sent: Tue 5/31/2016 3:11 PM

To: undisclosed-recipients:

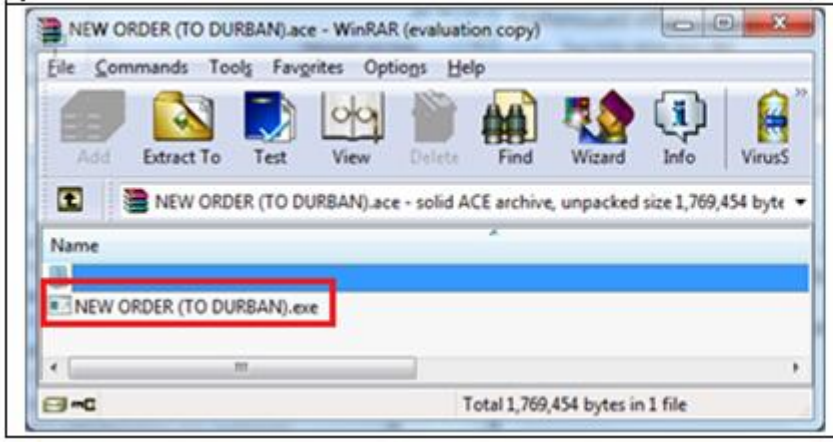
Message | NEW ORDER (TO DURBAN).ace (1 MB)

FYI
Dear Sir,

Find attach new arrivals for our market.
Kindly quote you be FOB Durban and include delivery time

Please need your quick comply.

Regards
Marcelo Morales



常見假冒郵件(釣魚網頁)

URGENT ATTN:common@nsshipmgt.com

Office Mail 365 [support_no_reply@office365.com]

Sent: Tue 5/17/2016 11:43 AM

To: [redacted]

You have (7) incoming e-mail pending and currently withheld by our sub-station due to e-mail/password server Authentication.

Click the link below to verify your email account Identity.

Verify Your Email Address

Failure to verify your email and password will result to email system failure and you will not be able to receive more mails henceforth.

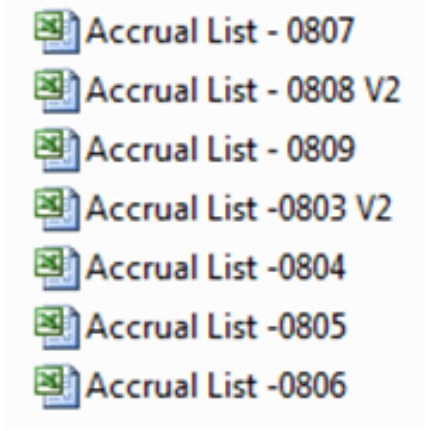
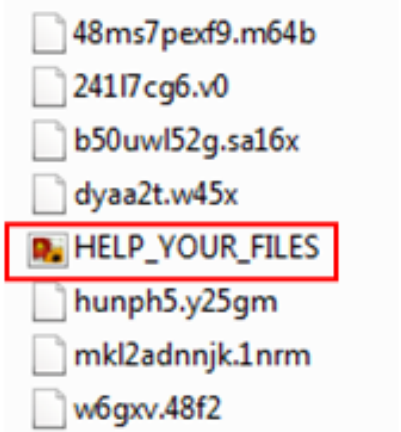
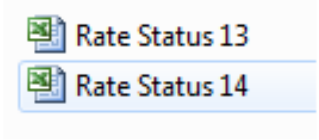
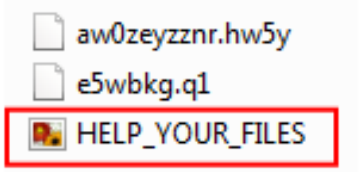
勒索軟體 (Ransomware)

- 通常透過木馬病毒的方式傳播，例如透過下載檔案夾帶，或是透過網路系統的漏洞而進入受害者的電腦。勒索軟體在進入後，會直接執行，或是透過網路下載病毒的實體數據，並恐嚇受害者。恐嚇訊息隨著不同的病毒而異，例如假借執法機關的名義，恐嚇受害者的電腦被發現進行非法行動，如色情、盜版媒體，或是非法的作業系統等。
- 某些實體數據只將作業系統鎖住，直到受害者付清贖金後才將電腦解鎖。實體數據可能以數種手段來達成恐嚇，包括將Windows的使用者介面（Windows Shell）綁定為病毒程式，或甚至修改磁碟的主啟動磁區、硬碟分割表等。最嚴重的一種實體數據將受害者的檔案加密，以多種加密方法讓受害者無法使用檔案，唯一的方法通常就是向該病毒的作者繳納贖金，換取加密金鑰，以解開加密檔案。
- 獲得贖金是這類病毒的最終目標。要讓病毒的開發者不易被執法單位發現，匿名的繳款管道是開發者的必要元素。有數種的管道發現被開發者用作匿名繳款，例如匯款、、數位貨幣比特幣等 (4-8 個) (大約港幣 5000 一個)。

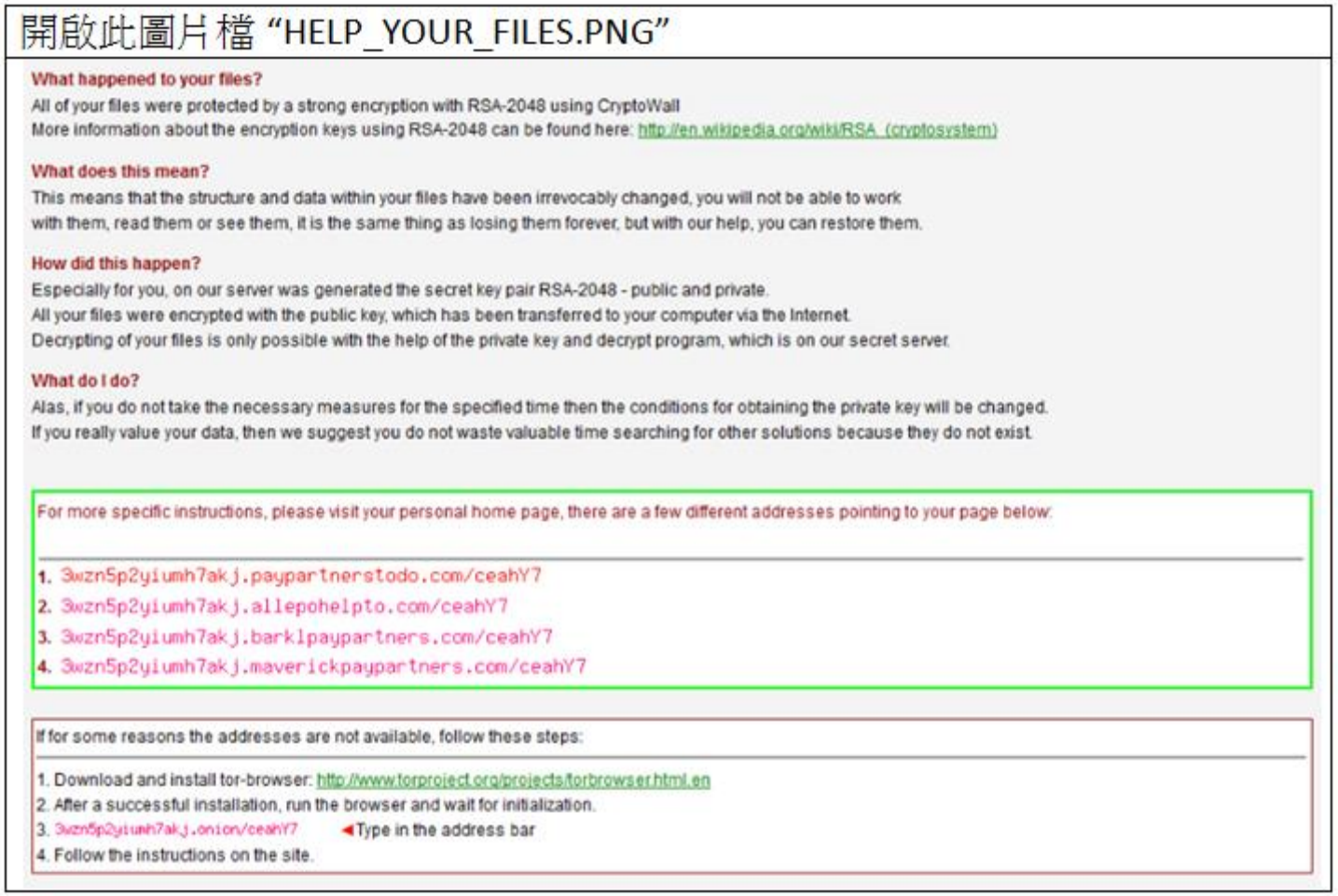
感染途徑

感染途徑示意圖：

勒索軟體特色(檔案加密)

未受勒索軟體感染之前的檔案	未受勒索軟體感染之後的檔案
	
未受勒索軟體感染之前的檔案	未受勒索軟體感染之後的檔案
	

勒索軟體特色(檔案加密)



開啟此圖片檔 “HELP_YOUR_FILES.PNG”

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - 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?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 3wzn5p2yiumh7akj.paypartnerstodo.com/ceahY7
2. 3wzn5p2yiumh7akj.allepohelpto.com/ceahY7
3. 3wzn5p2yiumh7akj.barklpaypartners.com/ceahY7
4. 3wzn5p2yiumh7akj.maverickpaypartners.com/ceahY7

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. 3wzn5p2yiumh7akj.onion/ceahY7 ◄Type in the address bar
4. Follow the instructions on the site.

勒索軟體解決方案

1. **防毒系統**：這是第一線的過濾機制，若能在郵件進入使用者信箱前先進行第一道的掃描，可以濾除多數能讓使用者植入勒索軟體的郵件。另外部份的防毒廠商（例如Kaspersky）有提供解密特定勒索軟體的工具。但不可輕易下載來路不明的疑似解密工具，使用後可能造成二次傷害，讓電腦被另一種勒索程式感染或被植入其他的惡意程式、木馬等等。
2. **定期進行檔案備份**：選擇具有保護備份檔案機制的備份系統，定期將檔案備份，可降低遭全硬碟型勒索軟體加密後的損失，也預防硬碟故障帶來的損失。
3. **對使用者教育訓練**：提高使用者對於勒索軟體的認知，降低因認知不足、好奇心或不好的操作習慣所帶來的損害。