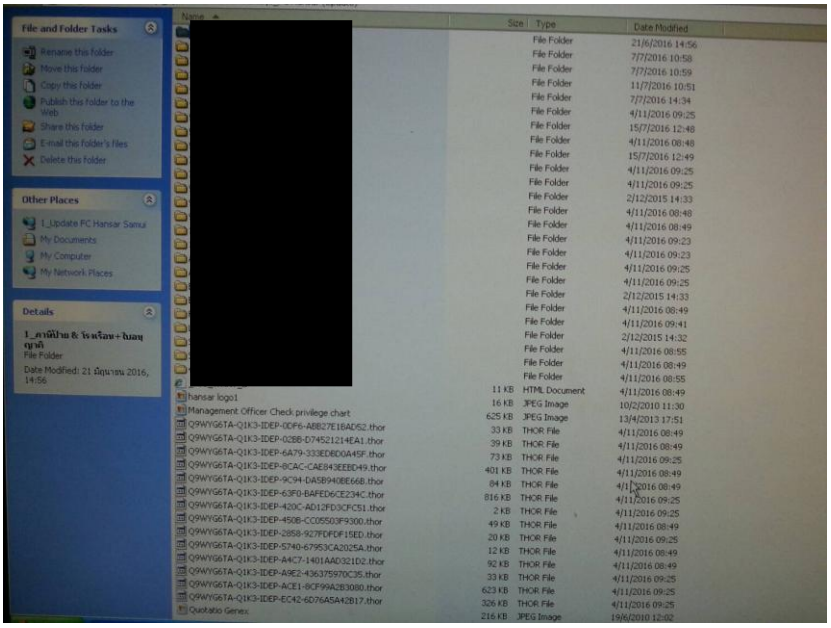
ความรู้เบื้องต้นเกี่ยวกับ Ransomware THOR

THOR เป็น Malware เวอร์ชั่นใหม่ล่าสุด คนไทยมักจะเรียกมันว่า “ไวรัสเรียกค่าไถ่” ที่กำลังแพร่ระบาดในปัจจุบัน โดยการทำงานของ Malware ตัวนี้ พบว่าจะถูกส่งมาทาง Email หรือ แฝงตัวมากับ Website ที่เข้าใช้งานต่างๆ หากผู้ใช้งานพลาดไปเปิดไฟล์ Malware ตัวนี้ ก็จะทำให้ไฟล์งานทั้งหมดถูกเข้ารหัสล็อคไฟล์ในทันที



รูปที่ 1.1 : ไฟล์งานที่ถูก Malware เข้ารหัส จะมีนามสกุลไฟล์เป็น .thor

การทำงานหลักๆ ของ Malware ตัวนี้คือ หากเปรียบเทียบการเข้ารหัสล็อคไฟล์ของ Malware ตัวนี้กับการปิดล็อคประตูบ้าน หากเราต้องการออกจากบ้าน เราก็จะต้องเอากุญแจ + แม่กุญแจ ไปล็อคเพื่อปิดประตูบ้าน แต่เมื่อไหร่ที่เราต้องการจะเปิดประตูบ้านเข้าไป เราก็จะต้องใช้ลูกกุญแจตัวเดิมในการไขแม่กุญแจเข้าไปได้

แต่ Malware ตัวนี้มีความพิเศษมากกว่านั้น กล่าวคือ เมื่อต้องการล็อคประตูบ้าน Malware ตัวนี้จะใช้ลูกกุญแจทั่วไป (Public Key) ในการล็อคประตู แต่เมื่อต้องการเข้าบ้านจะไม่สามารถใช้ลูกกุญแจเดิมในการไขเข้าบ้านได้ จะต้องใช้กุญแจพิเศษ (Private Key) เท่านั้นถึงจะไขกุญแจเปิดประตูเข้าบ้านได้

และที่สำคัญตัวถอดรหัสไฟล์นั้นมีความยาวของตัวอักษร, ตัวเลข และ อักขระพิเศษที่มีความยาวถึง 2,048 บิท (ตัวอักษร, หลัก) , (ขนาดรหัสผ่านที่เราตั้งๆ ใช้งานกันอยู่ หากเราตั้งที่ 8 หลัก ก็แทบจะจำกันไม่ได้แล้ว) ดังนั้นจึงยากที่จะสุ่มรหัสในการที่จะปลดล็อครหัสที่มีความยาวถึง 2,048 บิท (ตัวอักษร, หลัก) ได้

รูปที่ 1.2 : รูปแบบการเข้ารหัสล็อค และ การถอดรหัสไฟล์

วิธีการแก้ไข:

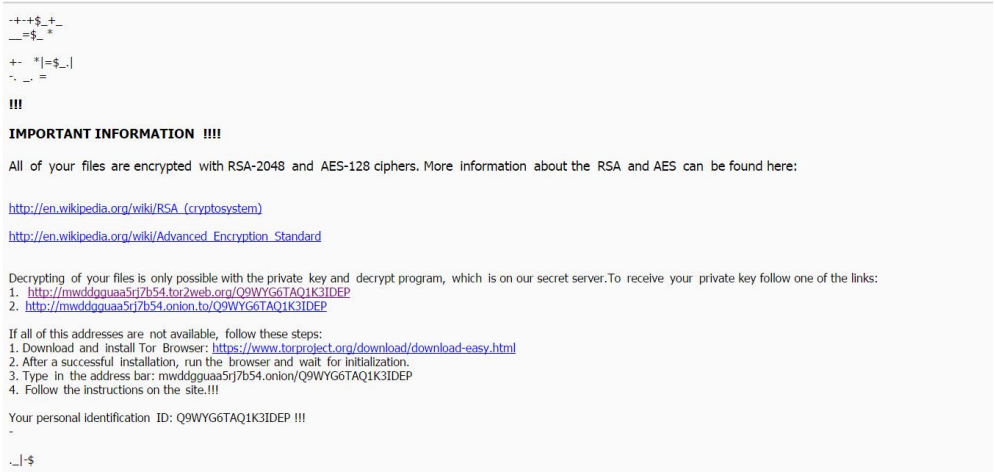
ณ.ขณะนี้ (08/02/17) ยังไม่พบวิธีการที่จะสามารถแก้ไข Malware ตัวนี้ได้เลย ดังนั้น จึงมีเพียง 2 แนวทางเท่านั้น ที่ให้เราเลือก คือ

1. ทิ้งข้อมูลทั้งหมด แล้วเริ่มใหม่

ถึงแม้ว่าคำตอบนี้จะดูเป็นคำตอบที่ออกแนวขวานผ่าซากซักหน่อย แต่ ณ.ปัจจุบันนี้ ยังไม่มีใครที่จะสามารถแก้ไข Malware ตัวนี้ได้จริงๆ

2. ตรงตามชื่อของมัน คือ ไวรัสเรียกค่าไถ่ ดังนั้นจะต้องมีการจ่ายค่าไถ่ไฟล์ก่อนถึงจะสามารถปลดล็อคได้

นอกจาก Malware ตัวนี้จะทำการล็อคไฟล์งานแล้วนั้นยังสร้างไฟล์ Auto Run ขึ้นมา เพื่อให้เราทราบได้ว่าจะต้องเข้าไปจ่ายเงินค่าไถ่ไฟล์ได้จากที่ใด


-+-+$_+_
__=$_*

+- *|=$_.|
-. _. =

!!!

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

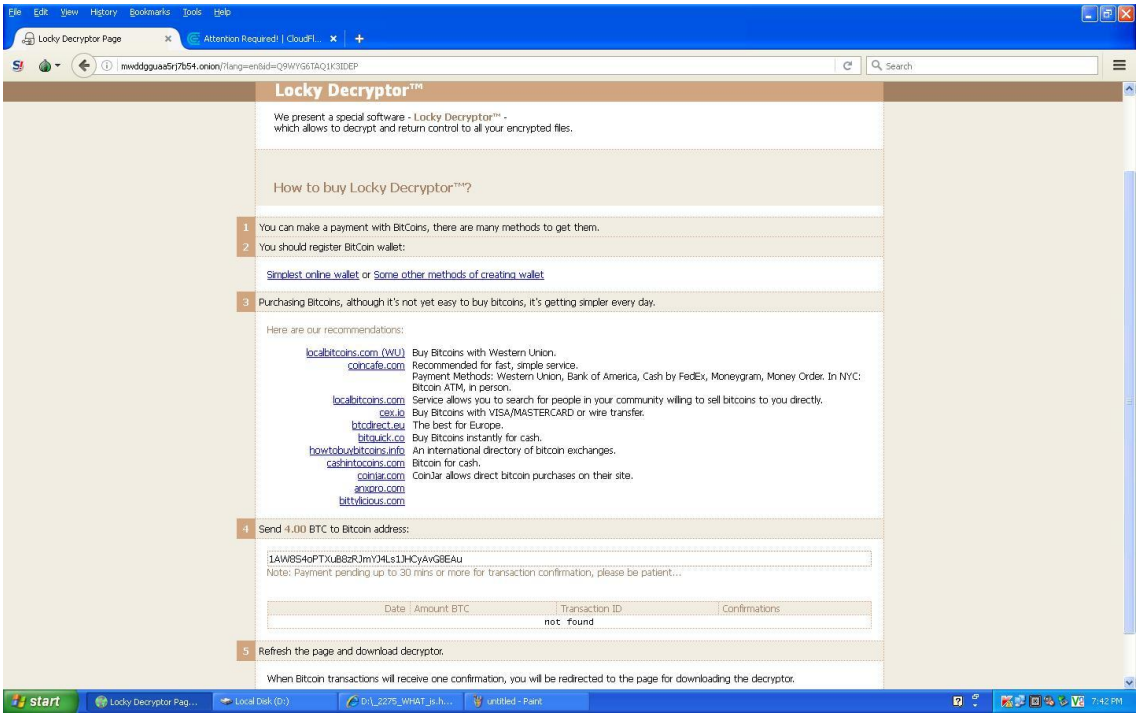
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.To receive your private key follow one of the links:
1. http://mwddgguaa5rj7b54.tor2web.org/Q9WYG6TAQ1K3IDEP
2. http://mwddgguaa5rj7b54.onion.to/Q9WYG6TAQ1K3IDEP

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: mwddgguaa5rj7b54.onion/Q9WYG6TAQ1K3IDEP
4. Follow the instructions on the site.!!!

Your personal identification ID: Q9WYG6TAQ1K3IDEP !!!
-

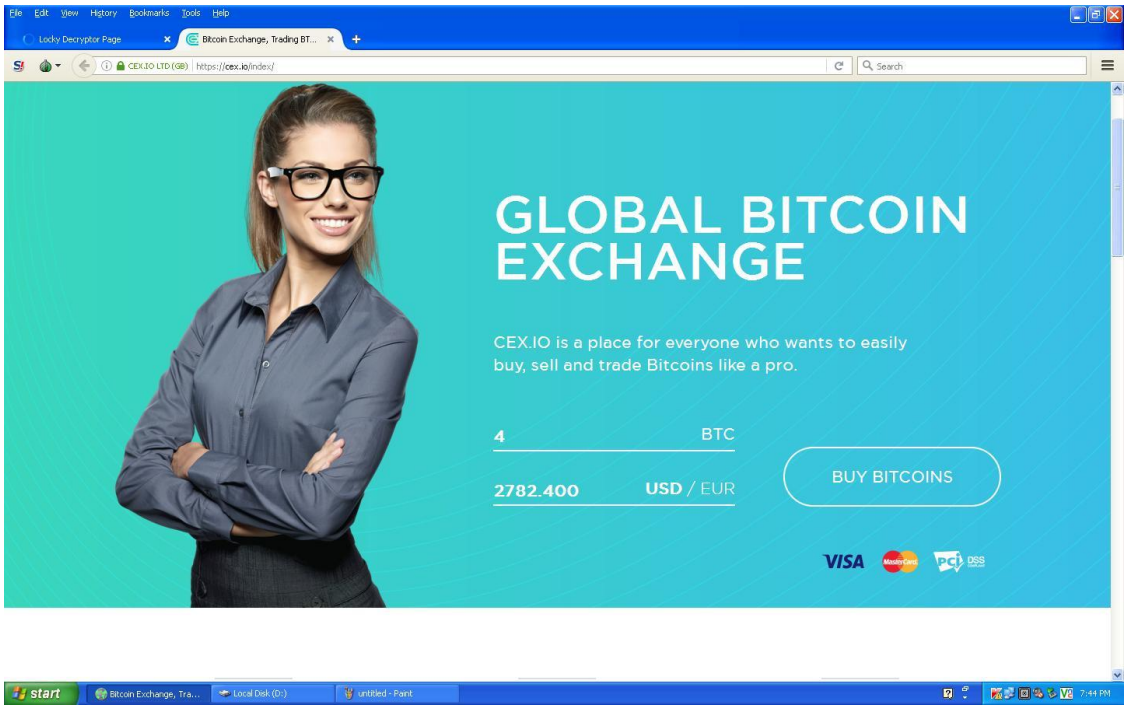
-_|-$

รูปที่ 1.3 : ไฟล์ที่ Auto Run ขึ้นมาเพื่อให้เราทำตามขั้นตอนการจ่ายค่าไถ่



รูปที่ 1.3 : รายละเอียด และ ช่องทางในการจ่ายเงิน

ในการจ่ายเงินนั้นจะต้องจ่ายเงินในรูปแบบ Bitcoins ซึ่งก็เป็นสกุลเงินจริงๆ นี่แหละครับ แต่การจ่ายเงินผ่าน Bitcoins นั้น จะทำให้ไม่สามารถแกะรอยไปถึงตัวผู้ที่รับเงินได้เลย



รูปที่ 1.4 : 1 การแปลง Bitcoins ให้เป็นสกุลเงินจริง

เทียบง่ายๆ ก็คล้ายๆ การแลกซื้อบัตรเติมเงินสดนั่นเอง โดย 1 Bitcoins จะมีค่าเท่ากับสกุลเงินจริงราว 704 ดอลล่าสหรัฐฯ (USD) โดยหากโดน Malware THOR เข้าไปจะถูกเรียกเก็บเป็นจำนวน 4 Bitcoins ก็ตกอยู่ที่ราว 2,783 ดอลล่าสหรัฐฯ (USD) หรือราวๆ 98,262 บาทไทย (THB)

ส่วนรูปแบบการจ่ายเงินเพื่อแลกเหรียญสามารถจ่ายผ่านบัตรเครดิต, เงินสด, โอนผ่านธนาคารระหว่างประเทศ ได้ทุกรูปแบบตามที่เขาได้แจ้งเอาไว้

จ่ายค่าไถ่ไปแล้วจะได้ไฟล์กลับมาไหม

ในข้อนี้ไม่มีใครสามารถการันตีได้ว่า หากเราได้ทำการจ่ายค่าไถ่ไปแล้วจะได้ไฟล์ที่โดนล็อคกลับมาหรือไม่ เพราะว่าการดำเนินการทั้งหมดกระทำผ่านโลกออนไลน์ทั้งสิ้น ซึ่งคนที่กระทำแบบนี้มีตัวตนอยู่บนโลกนี้จริง แต่ล่องหนในโลกออนไลน์ จึงทำให้ไม่สามารถระบุตัวตนของคนที่กระทำแบบนี้ได้ในโลกออนไลน์ จึงไม่มีอะไรการันตีได้เลยว่าจ่ายเงินไปแล้วเราจะได้ไฟล์กลับมา

สุดท้ายนี้ผมอยากบอกว่า ไม่มีอะไรที่ปลอดภัยได้ 100% บนโลกออนไลน์จริงๆ

เขียนบทความโดย: นายทวินันท์ วิริยะนานนท์ (Assistant IT Manager)

14 พฤศจิกายน 2559

HANSAR
SAMUI

TO:	All Hansarsamui Employees
CC:	Khun Rungthip (AHM)
Date:	February 08, 2017
From:	IT
Subject	Notification of Ransoms wear.

Dear All Staffs,

Currently there is a spam phishing email example below lure you to click the link in the email which after click the link, your computer might be infected with virus or spyware. Therefore, if you happen to receive this kind of email, PLEASE DO NOT CLICK LINK AND DELETE IT. Moreover, if you receive any strange emails, please forward to IT dept. for further investigation.

Please Forward mail to it@hansarsamui.com

Thank you appreciates your careful in this matter.

.

เรียน พนักงานทุกท่าน

ขณะนี้มีอีเมล์หลอกลวง หลอกให้ท่านคลิ๊กลิงค์ในอีเมล์ ซึ่งหากคลิ๊กลิงค์ดังกล่าวแล้ว อาจจะติดไวรัสหรือสปายแวร์ได้ ดังนั้นหากท่านได้รับอีเมล์ลักษณะดังกล่าวตามตัวอย่างด้านล่าง ห้ามคลิ๊กลิงค์ดังกล่าวและให้ลบอีเมล์นี้ หรือหากท่านได้รับอีเมล์ที่ไม่มั่นใจ กรุณา Forward มาให้ทาง IT ตรวจสอบก่อนคลิกทุกครั้ง

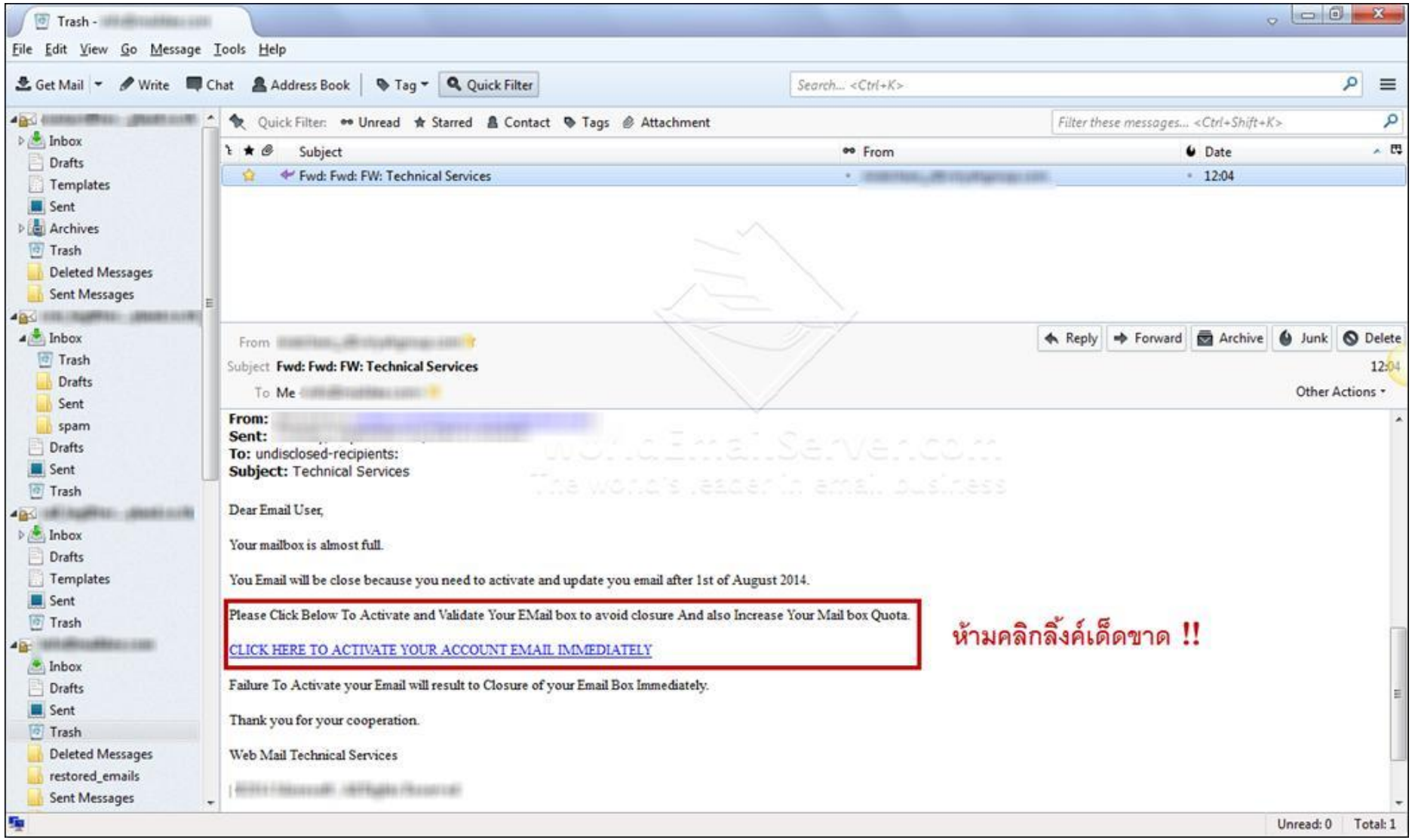
ส่งต่อเมล์มาที่ it@hansarsamui.com

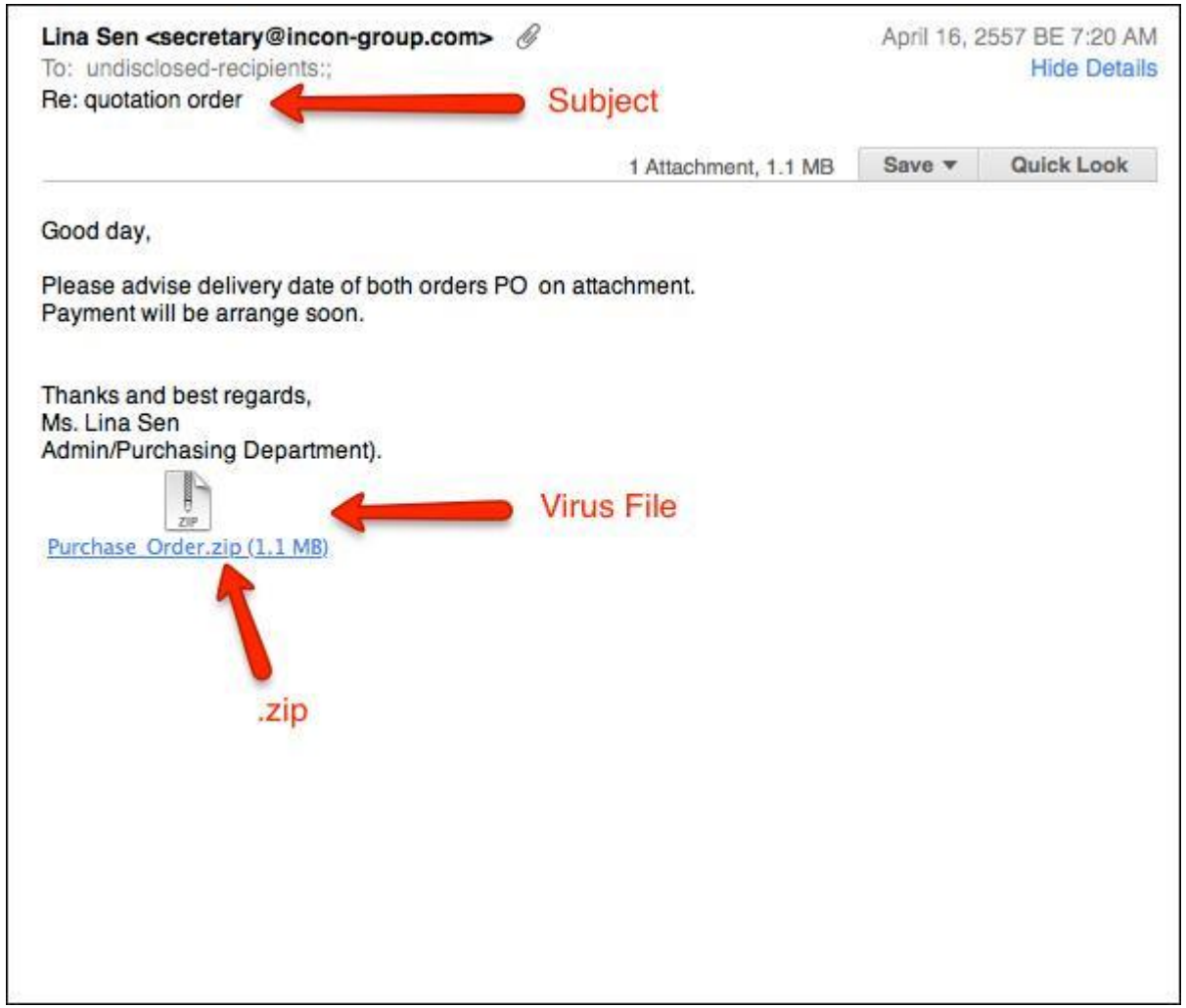
หากท่านโดนไวรัสหรือสปายแวร์แล้วนั้น จะไม่สามารถกู้ข้อมูลคืนมาได้

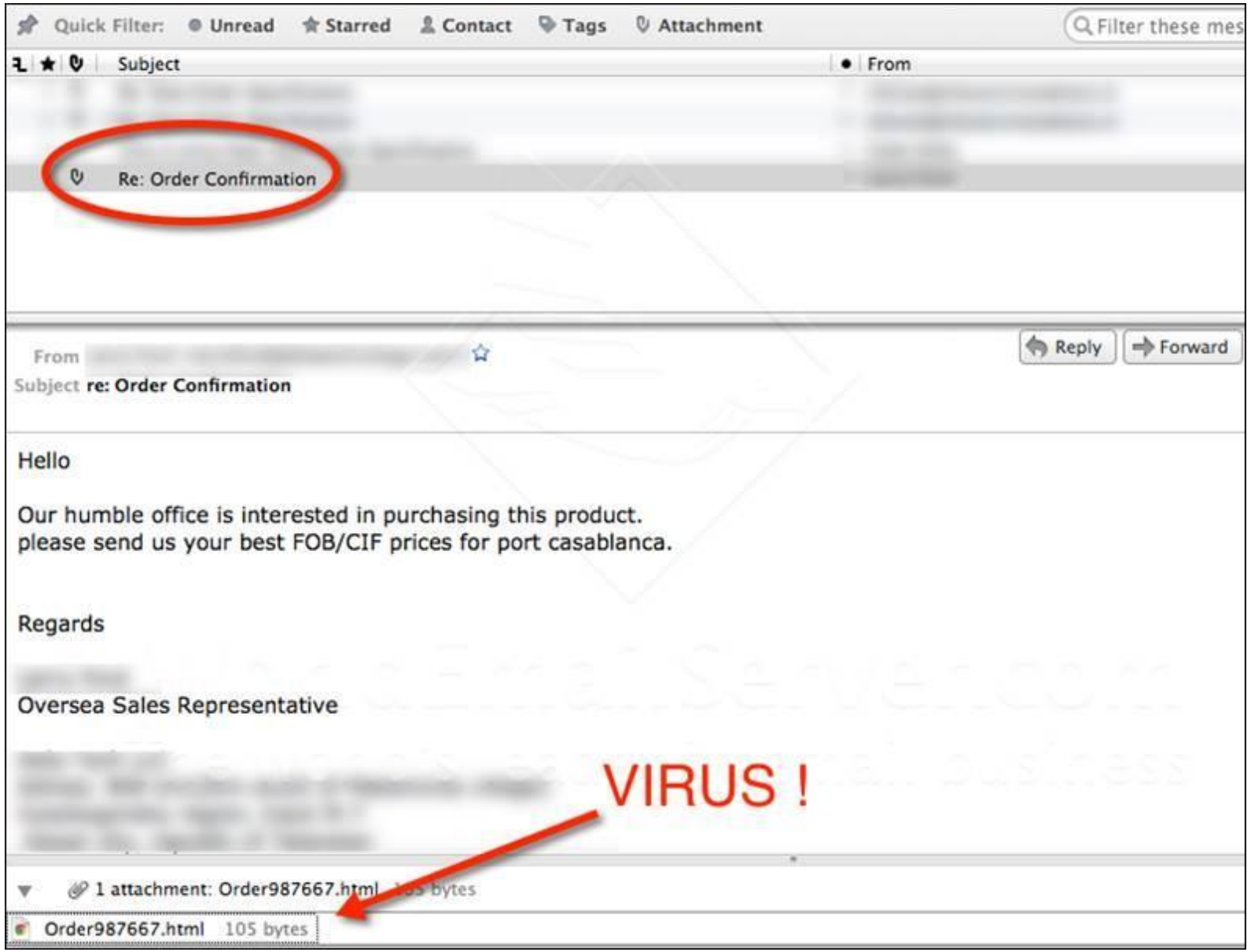
With best regards

Mr.Tawinun Wiriyananon
Assistant IT Manager
08 February 2017

101/28 Moo 1 Bophut
Koh Samui 84320 Thailand
+66 7724 5511
reservation@hansarmui.com.
www.hansarsamui.com


Trash -
File Edit View Go Message Tools Help
Get Mail Write Chat Address Book Tag Quick Filter
Search... <Ctrl+K>
Quick Filter: Unread Starred Contact Tags Attachment
Filter these messages... <Ctrl+Shift+K>
Subject From Date
Fwd: Fwd: FW: Technical Services 12:04
Inbox
Drafts
Templates
Sent
Archives
Trash
Deleted Messages
Sent Messages
Inbox
Trash
Drafts
Sent
spam
Drafts
Sent
Trash
Inbox
Drafts
Templates
Sent
Trash
Inbox
Drafts
Sent
Trash
Deleted Messages
restored_emails
Sent Messages
From
Subject Fwd: Fwd: FW: Technical Services
To Me
Reply Forward Archive Junk Delete
Other Actions
From:
Sent:
To: undisclosed-recipients:
Subject: Technical Services
Dear Email User,
Your mailbox is almost full.
You Email will be close because you need to activate and update you email after 1st of August 2014.
Please Click Below To Activate and Validate Your EMail box to avoid closure And also Increase Your Mail box Quota.
CLICK HERE TO ACTIVATE YOUR ACCOUNT EMAIL IMMEDIATELY
ห้ามคลิกลิ้งค์เด็ดขาด !!
Failure To Activate your Email will result to Closure of your Email Box Immediately.
Thank you for your cooperation.
Web Mail Technical Services
Unread: 0 Total: 1


Lina Sen <secretary@incon-group.com>
April 16, 2557 BE 7:20 AM
To: undisclosed-recipients:;
Hide Details
Re: quotation order
Subject
1 Attachment, 1.1 MB
Save
Quick Look
Good day,
Please advise delivery date of both orders PO on attachment.
Payment will be arrange soon.
Thanks and best regards,
Ms. Lina Sen
Admin/Purchasing Department).
Virus File
Purchase_Order.zip (1.1 MB)
.zip


Quick Filter:
Unread
Starred
Contact
Tags
Attachment
Filter these mes
Subject
From
Re: Order Confirmation
From
Subject re: Order Confirmation
Reply
Forward
Hello
Our humble office is interested in purchasing this product.
please send us your best FOB/CIF prices for port casablanca.
Regards
Oversea Sales Representative
VIRUS !
1 attachment: Order987667.html
Order987667.html 105 bytes