

Ransom ware - what is it ?

Trends in Malware

Ransom ware – how it works

How could I get it ?

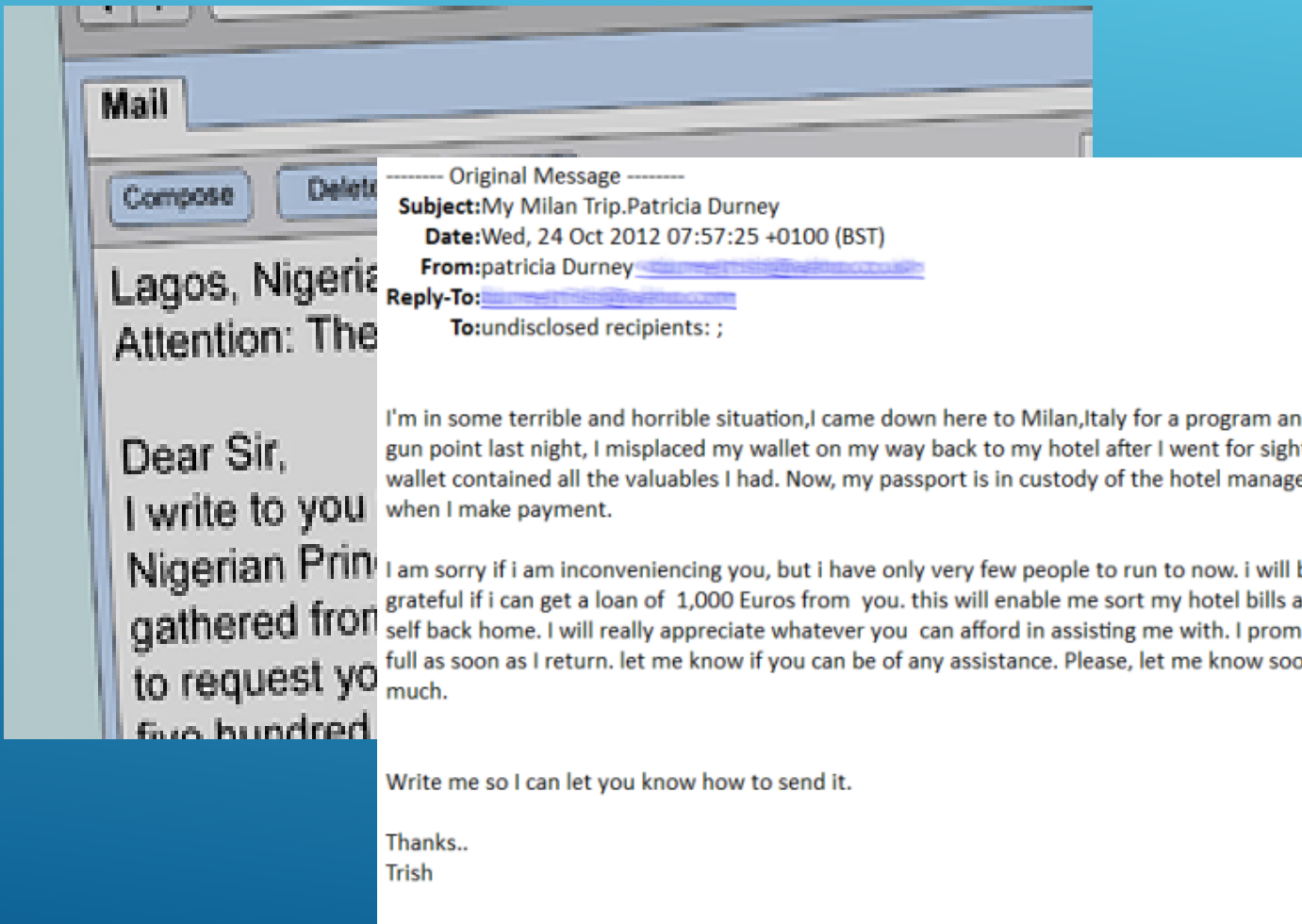
Recovery -- Bit Coins payment

-- Restore from Backup

Malware Trends

- ▶ **Stage One - a virus to achieve notoriety or seek assistances**
Anti-Virus protection, Educate the Gullible (Nigerian etc)
- ▶ **Stage Two - capturing Banking or Credit Card details**
Banks aware of perpetrators and block transfers
Money laundering needed - via gullible third parties
- ▶ **Stage Three – crypto locking key data, seeking ransom money**
Ransom payable in untraceable Bit-Coins
Targeting small business, with 'viable' emails

Scammers to the Gullible



[Web Version](#) | [Update preferences](#) | [Unsubscribe](#)



DHL notification

Our company's courier couldn't make the delivery of parcel.

REASON: Postal code contains an error.
LOCATION OF YOUR PARCEL: New York
DELIVERY STATUS: sort order
SERVICE: One-day Shipping
NUMBER OF YOUR PARCEL: ETBAKPRSU3
FEATURES: No

Label is enclosed to the letter.
Print a label and show it at your post office.

An additional information:

If the parcel isn't received within 15 working days our company will have the right to claim compensation from you for it's keeping in the amount of \$8.26 for each day of keeping of it.

You can find the information about the procedure and conditions of parcels keeping in the nearest office.

Thank you for using our services.
DHL Global

[Edit your subscription](#) | [Unsubscribe](#)

Getting Banking Details



PROTECTING YOUR ACCOUNT

Our Technical Service department has recently updated our online services, and due to this upgrade we sincerely call your attention to follow below link and reconfirm your online banking account details. Failure to confirm your ANZ online banking account details will permanently suspend you from accessing your account online.

<http://www.anz.com.au/INETBANK/bankmain.asp?action=update>

We use the latest security measures to ensure that your online banking account is safe and secure. The administration asks you to accept our apologies for the inconvenience caused and expresses gratitude for cooperation.


J. A. Smith
Security Advisor
ANZ Online Banking

A screenshot of the ANZ Internet Banking Update page. The page has a blue header with the ANZ logo on the left and 'help | print' on the right. Below the header, the text 'Welcome to ANZ Internet Banking Update' is centered. The main content area is a light gray box containing several input fields: 'Card Holder Name', 'Credit Card Number', and 'Password', each with a question mark icon to its left and a text input field to its right. Below these is a text prompt: 'If you were referred by an ANZ Staff Member, please enter the Referral Code.' followed by a 'Referral Code' label and a text input field. A blue 'log on' button is positioned to the right of the Referral Code field. At the bottom of the gray box, there is a link: '* [Software Requirements and Settings Guide](#)'. Below the gray box, there is a note: 'If you do not have a Customer Registration Number and Telcode, please call 13 33 50 (option 1) 24 hours a day, 7 days a week.' and another note: 'Note: While using ANZ Internet Banking, please do not use your browser's BACK button.'

Bogus Website – gets Acct details

Crypto-Locker Examples

WA Appliance Parts: Delivery Exception E-mail Reference 019408
AusPost E-Tracker <shadowofraven0121@yahoo.com>
Sent: Fri 4/03/2016 6:56 AM
To: Parts
Message WA Appliance Parts_AusPost Tracking Label_id00-my4qb18j.zip (2 KB)



Delivery Exception
Address Update Required

Hi, your parcel has experienced an exception.

Shipment Details

TRACKING #	AU162701661
SENT TO	WA Appliance Parts
ADDRESS	4/ 209 Winton Road, Joondalup, WA, 6027

Example:

AGL electricity account.

Once clicked, damage starts

Small Business Examples

From: "Mike Evans" <heidinichols@att.net>
Subject: Reminder: Your unpaid bill 16M-250529 requires instant reaction
To: beast@melbpc.org.au

Attention to the finance department.

This letter is to remind you that invoice number **001496833** is overdue.
The amount of **AUS 1,986.00** should have been sent by 24 of March 2016.

Kindly confirm the receipt of this confirmation.
Shall you need assistance or have questions about this letter,
[please contact me immediately](#)

Your business is greatly appreciated!

Mike Evans

Billing and Collection

Patricia Spratt For The Home

A.B.N 34832526321

[Sydney, New South Wales, 2000](#)



[beast_INV16-07544.doc](#)

Tend to arrive 9am-10am local time!

From: Richard [Laslett](#) <cjirsa@cox.net>
To: East SIG <east@melbpc.org.au>
Subject: east, Your refund has been wired R001243380

Dear east,

We are writing to confirm that the refund for Order no. **MAR/0603727** in the amount of **\$ 2,694.00** has been [remitted](#) back to your account **today**. Kindly see the attached [document](#) for details about the transaction.

Please don't hesitate to contact me if anything's unclear or [further questions](#) exist.

[Richard Laslett](#) | Accounting Management
Orville Platt High School | +61.08.9258.4855
[Darra, Queensland, 4076](#)



[east_01-6-161.doc](#)

What Happens ?

- Needs “click” to open / activate
- Virus encrypts documents, pics, music etc
- Looks at all drives, including networks
- May give “progress” message
(we are now getting your details)
- Data can only be retrieved using a
specific decryption key
- Ransom demand to get the needed key

The screenshot shows a website for buying decryption services. At the top, there is a navigation bar with links for 'Buy Decryption', 'Decrypt Single File' (with a 'free' tag), 'FAQ', and 'Support'. The main heading is 'Buy decryption and get all your files back'. Below this, a yellow-bordered box contains the following information: 'Buy decryption for 399 EUR before 2015-05-12 10:47:13', 'OR buy it later with the price of 798 EUR', 'Time left before price increase: 94:25:40', and 'Your total files encrypted: 3048'. Below the box, it shows 'Current price: 1.9791198 BTC (around 399 EUR)', 'Paid until now: 0 BTC (around 0 EUR)', and 'Remaining amount: 1.9791198 BTC (around 399 EUR)'. Underneath, the text 'Buy Decryption with' is followed by a numbered list: '1 Register bitcoin wallet' and '2 Buy bitcoins'. Below step 1, it says 'You should register Bitcoin wallet, see [easy instructions](#) or [watch video](#) on YouTube.' Below step 2, it says 'Please see recommended bitcoin sellers in your country:' followed by four links: 'www.eircoin.net - Order bitcoin with AIB bank transfer.', 'www.bitstamp.net - Buy and sell bitcoins in european SEPA zone', 'localbitcoins.com - Buy Bitcoins with cash from people leaving in Ireland.', and 'howtobuybitcoins.info - Big list of trusted Bitcoin online exchanges in Ireland.'

Your personal files are encrypted by CTB-Locker.



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95 59 01

Next >>



[View encrypted files](#)

Time until costs raise

23:57:21

Costs: btc

Paid: btc

[Check payment and receive keys](#)

Key: IV:

[Decrypt using keys](#)

30gb of personal documents and files on this computer or device have just been encrypted. Encrypted means you will not be able to access your files anymore, until they are decrypted. Your original files have been deleted, these can be recovered as described below. Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-128). The only way to decrypt your files, is to obtain your private key and IV.

The private key, which will allow you to decrypt and get your original files back, is stored on our server. Each time the timer hits zero, the total costs will raise with the starting price.

To receive your private key, you need to pay the amount of bitcoin displayed left of this window (costs).

You need to send the amount of bitcoins to the bitcoin address at the bottom of this window.

After the purchase is made, please wait a few minutes for confirmation of the bitcoins. After the bitcoins are confirmed, click the 'check payment and receive keys' button. Your keys will appear in the textboxes. After that, you simply click 'decrypt using keys', your files will be decrypted and restored to their original location.

You can easily delete this software, but know that without it, you will never be able to get your original files back.

For more information on how to buy and send bitcoin, click 'Next page'.

[<< Previous Page](#)

[Next Page >>](#)

HOW TO USE BITCOINS



Open an account on Circle, Coinbase, LocalBitCoins. This gives you the basic facilities to send, receive, and store



Your account on one of these bitcoin hosts will provide you a unique string of letter and



Buy Bitcoins with a standard offline currency, either from a bank transfer, cash, or credit card payment. Your new digital funds are added to your wallet.



 **bitcoin**
ACCEPTED HERE



SUBWAY
eat fresh.®



Recovery

- **PAY UP** - \$300 - \$600 (using Bit Coins !)
 - No guarantee key will be provided, or that it will work 100%
 - Still need to remove the virus to stop re-infection, 2nd Hit
- **OR Use Image Restore** - may need to go back a few days/weeks
 - Trade-off – Delayed Encryption (to infiltrate backups vs exposure)

Summary

- ▶ Ransomware becoming major risk for all computing, targeting individuals and Small Business
- ▶ Social Engineering concepts being exploited – for the Gullible
- ▶ Critical that we have good Off-line backups (and tested..)
- ▶ Good housekeeping - Don't open unsolicited or copycat emails
be wary of mock or known problem websites / material
- ▶ Overall education needed . . . Family, Staff etc