

# A Case Study

Presented by Mick Jameison.



A Five Year Investigation

- A Global Organised Crime Group.

Victims in two Continents

- Losses exceeding \$250 Millions

Suspects in four Continents

- International cooperation between law enforcement agencies.

DETAILS OF THIS PRESENTATION WILL INCLUDE

- Report of an unlawful access to computer servers was made by a credit card company – April 2008.
- A payment processor was identified as a Point of Compromise
- A private company was employed to deal with Technical Examination of the servers.
- Losses by this single breach exceeded \$US 25 Million.

**UK Authorities receive an allegation of Cyber Crime.**



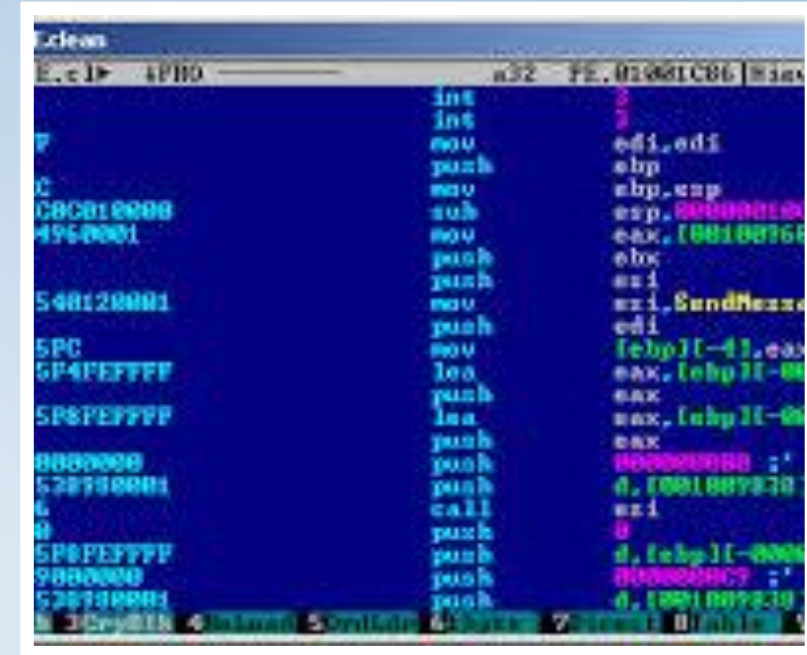
# Data Breach



- Reported to Cyber Crime Unit - April 2008
- Breach investigated by private company
- SQL injection
- Later by Malware



Malware examination indicated that the suspects used email addresses in Vietnam.



The image shows a debugger window with assembly code. The code includes instructions like 'int', 'push', 'mov', 'sub', 'xor', 'lea', and 'call'. Some values are highlighted in pink, such as '00000000' and '00000001'. The window title is 'x64dbg' and the address is '00401000'.

Matching Signatures
Printf formatting strings found in memory and binary data
Queries a list of all running processes
Urls found in memory or binary data
Binary may include packed or crypted data
Downloads files from webservers via HTTP
Performs DNS lookups
Queries the product ID of Windows
Contains capabilities to detect virtual machines

# Criminal forums.



## VISA classic, MC, Cirrus, Maestro, Electron:

>250\$ one time payment - 12\$ one dump  
>1500\$ one time payment - 8\$ one dump  
>5000\$ one time payment - 5\$ one dump

## VISA gold/platinum, Discover, Dinners, AmEx:

>250\$ one time payment - 30\$ one dump  
>1500\$ one time payment - 20\$ one dump  
>5000\$ one time payment - 10\$ one dump

EU (min order 1000\$)

## VISA classic

80\$ one dump

## VISA gold/platinum

160\$ one dump

## MasterCard

110\$ one dump

## Amex

100\$ one dump

EU (min order 1000\$)

## VISA classic

80\$ one dump

## VISA gold/platinum

160\$ one dump

## MasterCard

110\$ one dump

If you need known balance on card price + 50%

\* France, Spain and Italy dumps price: gold 170\$, classic 110\$, mc 130\$

## Rules:

You can order checked, or unchecked dumps, if you choose unchecked i will give +20% bonus. I dont care if there is No-Money. I replace only Pick-Up codes. Best way if you check dumps yourself and i replace bad ones immediately. I dont replace unchecked stuff. If you need KnownBalance on card, price will be + 50%.

## Payment:

I accept WebMoney. You can make exchange here: USD -> WMZ , E-Gold -> WMZ. From good and well-known clients i can accept WU and MG payments. [/b]

PROFILE

PM

WWW

ICQ

Display posts from previous:

All Posts



Oldest First



Go

# Covert Investigation



- Undercover assets employed.
- Credit card accounts recovered
- Suspects IP addresses identified.



# Vietnam

- IP addresses resolved to Vietnam on 14/05/2008.
- The UK requests assistance from the Vietnam Hi-Tech Crime Unit 13/06/2008





# Vietnam

- Vietnamese Legislation Difficulties.
- Vietnamese commenced Money Laundering Investigation.



# Vietnam has no legislation to deal with UK request

- No offence for hackers inside Vietnam to attack servers outside it's borders.
- Advice given to the Hi Tech Crime Unit to create the legislation.
- On 01/01/2011 new cyber legislation came into force in Vietnam

# Vietnam Money Laundering Investigation

- \$280,000 Western Union Transfers to 6 suspects.
- DISC supplied to SOCA with all transactions seeking further evidence.



## SOCA – Vietnam (Disc)



- 2,077 transactions in total.
- 1,389 Money transfers from UK.
- 1,359 supplied false information when sending money. (Further Arrests?)
- Evidence from voters register.
- 50 Witness statements provided



# **SOCA – London Arrests.**

- Fraud identified at Stagebeat.
- sibna22@yahoo.com
- 78 Albatross Close, London  
E6 5NX

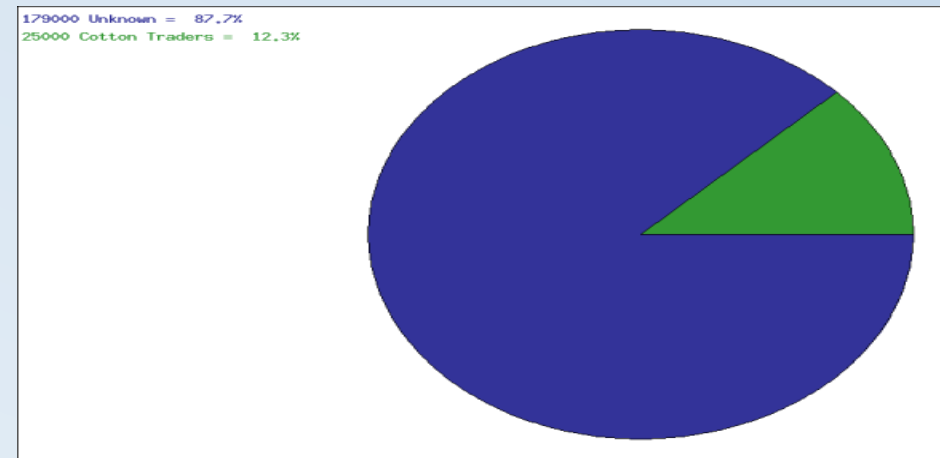


- Preservation Order on e-mails on 14/07/2008
- E-mails received from Yahoo - USA on 23/04/2009
- Vietnamese suspects e-mail accounts (204,000 credit cards) – **mattfeuter**
- Egyptian suspects e-mail accounts (18,000 credit cards) – **menem99**

London Arrests – e-mails

# Credit Card Research.

- 25,000 credit cards (approx) from identified victim.
- Remainder - Unknown



# London arrests -Search

- Two prisoners.
- Five computers containing over 800 card details.
- Forged identification documents.
- On-line fraud.





# London Arrests - Prisoners

- Gboyega AKINBOLA.
- AKA – sibna22, lopey14,
- Oyetunde OYEDEJI.
- AKA – teedazzles, candidman, lopey14
- Subsequently sentenced to two and half years imprisonment.



## London Arrests

- Phone and e-mail links to suspects in Vietnam and Egypt.
- Western Union Transfers – Sibna Khanom to Egypt and Vietnam (Not on disc).



# London Arrests – Egypt.

- SOCA intelligence research.
- Memengg is Abdelmonim ABOELMAGD
- Letter of Request sent to Egypt
- Investigation commenced in Egypt 9<sup>th</sup> June 2009.
- Investigation concluded December 2009 – suspect claimed emails had been hacked.
- No forensic examination of computers.

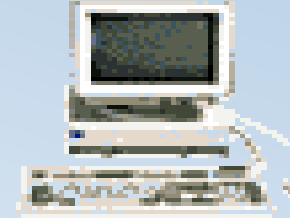




# London Arrests – Links



← Supply of credit cards to Becton Suspects.



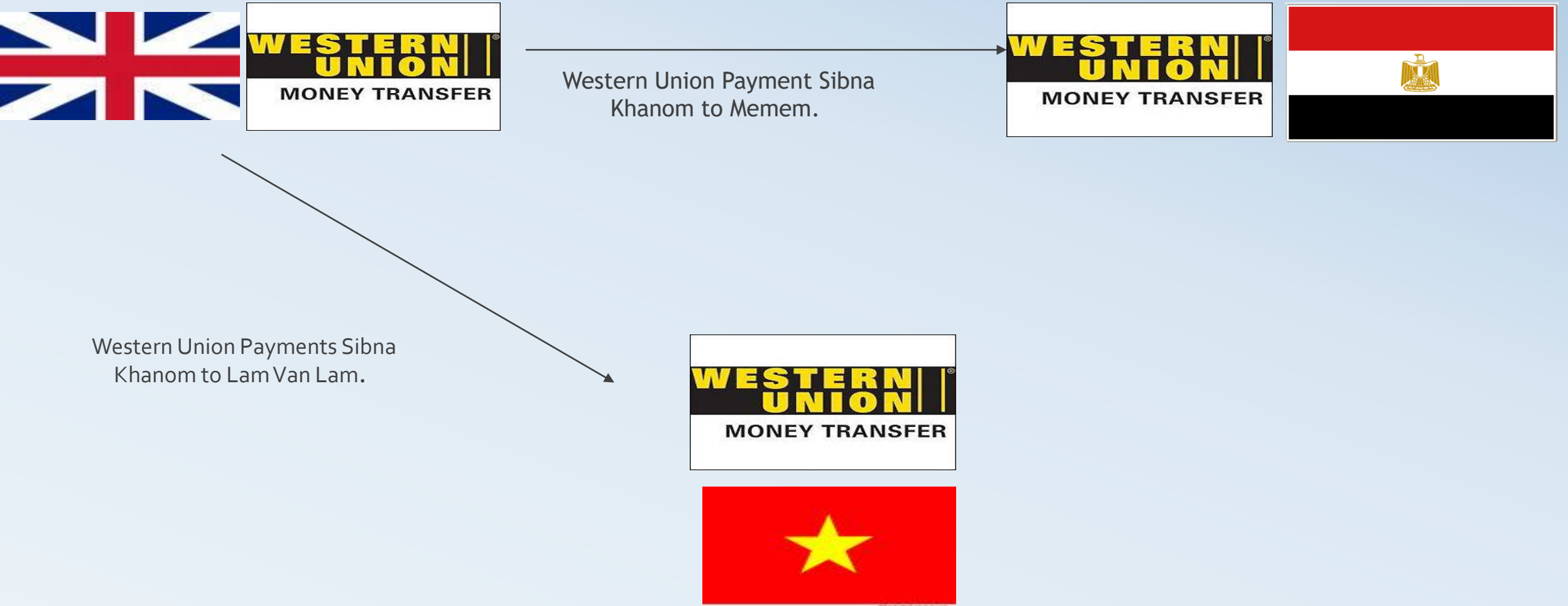
Supply of credit cards to Menem99.

Supply of credit cards to London Suspects.





# London Arrests – Links



## Four Vietnamese youth found hacking UK credit cards 12/21/2010 12:30

Vietnam's hi-tech crimes investigation department Monday said that they have busted a ring of Vietnamese hackers who had used 100,000 credit cards in the UK, pocketing billions of dong.

Le Dang Khoa, Nguyen Ngoc Lam, Nguyen Ngoc Thanh and Nguyen Dinh Nghia belonging to Ho Chi Minh City and Hanoi, joined hands with some foreigners to hack the system of a UK company to steal security information on the credit cards worth 6 million pounds (US\$9.32 million) in total.

The screenshot shows a web browser window displaying the Thanh Nien News website. The browser's address bar shows the URL <http://www.thanhniennews.com/2010/pages/2010122>. The website's header features the "THANH NIEN NEWS .com" logo and the tagline "Latest news & information about Vietnam". Navigation links for "Home", "Vietnamese Edition", and "About us" are visible. A search bar is located on the right side of the header. The date and time "Wednesday, October 23, 2013 13:30" are displayed in the top right corner. A sidebar on the left lists various news categories: POLITICS, BUSINESS, SOCIETY, YOUTH / SCIENCE, SPORTS, ENTERTAINMENT / ARTS, TRAVEL, HEALTH, WORLD / REGION, SPECIAL REPORT, and COMMENTARIES. The main content area features a news article titled "Four Vietnamese youth found hacking UK credit cards", which was last updated on Tuesday, December 21, 2010, at 12:30. The article includes a photograph of several credit cards (MasterCard, Visa, and a bank card) and text stating that Vietnam's hi-tech crimes investigation department has busted a ring of Vietnamese hackers who used 100,000 credit cards in the UK, pocketing billions of dong. The article also mentions that the busting operation was conducted in cooperation with the UK police, led by Nguyen Thanh Hoa, chief of the department (C50) under the Ministry of Public Security. The article text continues: "Le Dang Khoa, Nguyen Ngoc Lam, Nguyen Ngoc Thanh and Nguyen Dinh Nghia belonging to Ho Chi Minh City and Hanoi, joined hands with some foreigners to hack the system of a UK company to steal security information on the credit cards worth 6 million pounds (US\$9.32 million) in total." To the right of the article is a "Latest news" section with a list of recent headlines, including "Vietnamese forces put out fire on stranded Vanuatuan ship", "Abbott donates VND5 billion in products to support typhoon relief efforts", "In Vietnam, genetically modified crops set to get official green light", "Violations found in building of \$30,000 school toilets in central Vietnam", and "Hanoi hosts two international film fests". At the bottom right, there is a social media widget for "Thanh Nien News" showing a Facebook "Like" button with 5,663 likes. The Windows taskbar at the bottom of the screen shows various application icons and the system clock indicating 13:30 on 23/10/2013.

http://www.thanhniennews.com/2010/pages/2010122

Vietnam latest news - Than...

File Edit View Favorites Tools Help

McAfee

SONY

15°

bing

SEARCH

ADVERTISEMENT

THANH NIEN NEWS .com

Latest news & information about Vietnam

Home Vietnamese Edition About us

Search

Wednesday, October 23, 2013 13:30

POLITICS

BUSINESS

SOCIETY

YOUTH / SCIENCE

SPORTS

ENTERTAINMENT / ARTS

TRAVEL

HEALTH

WORLD / REGION

SPECIAL REPORT

COMMENTARIES

Four Vietnamese youth found hacking UK credit cards

Last updated: Tuesday, December 21, 2010 12:30

Vietnam's hi-tech crimes investigation department Monday said that they have busted a ring of Vietnamese hackers who had used 100,000 credit cards in the UK, pocketing billions of dong.

The busting operation was conducted in cooperation with the UK police, said Nguyen Thanh Hoa, chief of the department (C50) under the Ministry of Public Security.

Le Dang Khoa, Nguyen Ngoc Lam, Nguyen Ngoc Thanh and Nguyen Dinh Nghia belonging to Ho Chi Minh City and Hanoi, joined hands with some foreigners to hack the system of a UK company to steal security information on the credit cards worth 6 million pounds (US\$9.32 million) in total.

Latest news

- Vietnamese forces put out fire on stranded Vanuatuan ship
- Abbott donates VND5 billion in products to support typhoon relief efforts
- In Vietnam, genetically modified crops set to get official green light
- Violations found in building of \$30,000 school toilets in central Vietnam
- Hanoi hosts two international film fests

Vietweek Thanh Nien News

Like 5,663

Thanh Nien News

13:30 23/10/2013

# Summary to date of investigation end 2010.

- Prosecutions in United Kingdom.
- Investigations in Egypt and Vietnam failed.
- Support to Vietnam of Cyber Legislation.
- Capability Building agreements with Vietnam.

# Mattfeuter – New Investigation from 2011

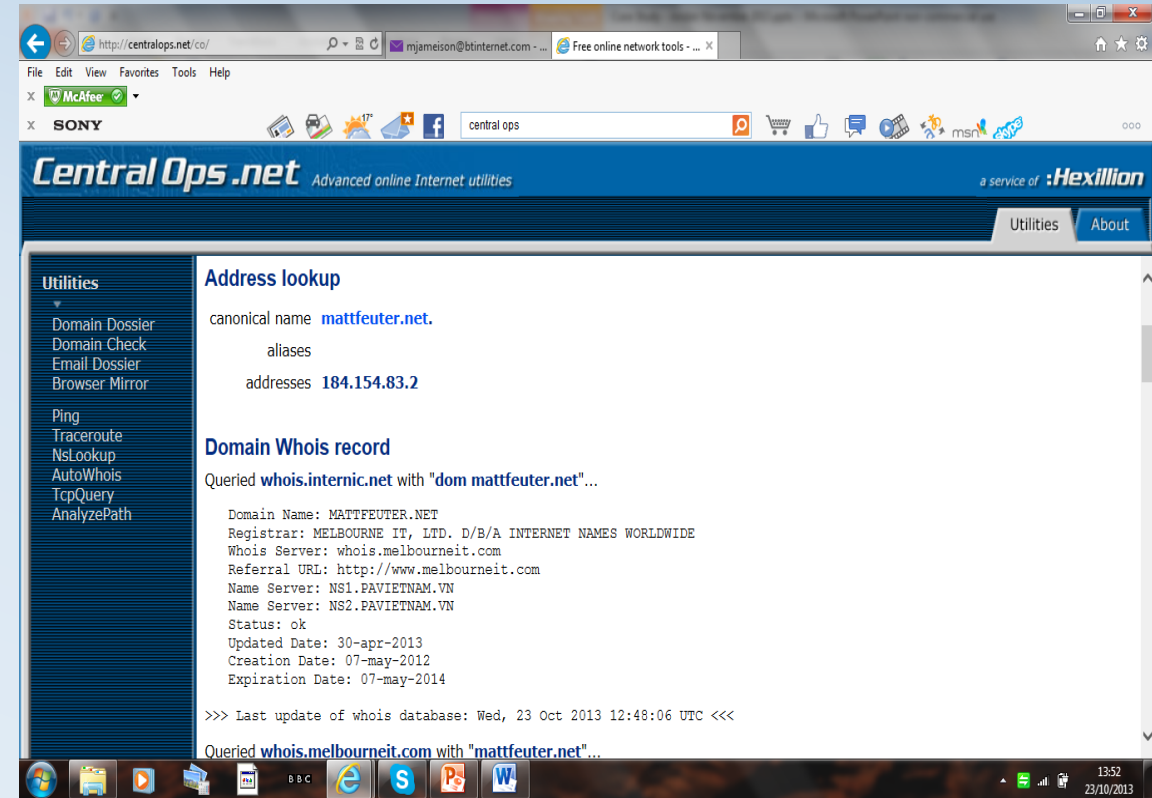
- Mattfeuter continued to operate.
- Further investigations began in the UK in Partnership with USA.
- Vietnam agreed to commence investigation so long as evidence was after 01/01/2011





# New Operation – First Steps

- The registration of the website Mattfeuter was examined.
- Enquiries into the Domain Name Registrant revealed a name of Van Tien Tu.



# New Operation – First Steps

- Test Purchases of Credit cards.
- Revealed email addresses of suspects.
- Identified methods of payments had changed.
- Demonstrated that the criminal group remained in place



# VIRTUAL PAYMENT SYSTEMS



Exchanger



# Gathering Evidence



- Joint investigation with FBI revealed all email content.
- This identified the suspects.
- Joint report was prepared and sent to Vietnam.
- Evidence demonstrating over US\$200Million losses and 1.1 Million credit cards sold.





# Vietnamese investigation.

- Received report and analysed emails.
- Resolved IP addresses
- Located suspects and used conventional surveillance.
- Financial investigations.





## Vietnamese arrests – June 2013

- **Van Tien TU** – Site Owner and head of Mattfeuter
- **Truong HAI DUY** – Site administrator for three years till end 2012
- **Le Van KIEU** – Site administrator from end 2012



# Vietnamese arrests - Financial

- Luxurious Lifestyle.
- Significant assets recovered.



## Results of Interviews.

Van Tan Tieu took over the control of Mattfeuter in 2008.

They obtained the credit cards details from Eastern European Hackers.

They bought the cards for around US\$1 each.

They sold the cards for US\$2 – 15 each.

They sold between 50 to 250 cards everyday.

The administrator received a salary.

Van Tan Tieu kept the profits.



# Some online reports of the case.





Any Questions  
Thank you!

