DE ROOS & PEN

IBA Annual Conference 2013 – Lecture on Cybercrime

- A wise man told me yesterday in the taxi that using a powerpoint made the audience lazy
- People don't have to listen anymore, because they can read
- I hope to prove him wrong
- Cybercrime very interesting part of criminal law
- Hard to keep up
- Playground for criminals
- Finding new ways to make money
- So much data stored, imposes giant risks, not only privacy risks.

Sheet 1

- To make an example, this is old school
- Insert gas in ATM so it explodes
- They ram the ATM with a car and steal the money
- Dangerous heist, suspects are known to have lost arms and legs
- Average profit around 50 thousand euro's

Sheet 2

- ATM Heist may 2013
- 45 million dollar theft
- Drain cash machines around the world (mostly the US /NY) in just over 10 hours
- 36.000 transactions
- Broke into credit card processors,
    - increased available balance and withdrawal limits on prepaid Credit Cards,
    - distributed counterfeit cards to 'cashers' who drained cash machines.
- Although they are criminals, I have a lot of respect for the level of sophistication
- Next level: hacking in ATM's to make ATM's spit out money

CRIMINAL DEFENCE LAWYERS

Keizersgracht 332
1016 EZ Amsterdam

T +31 (0)20 627 5411
F +31 (0)20 622 6577

E info@deroosenpen.nl
I www.deroosenpen.nl

DE ROOS & PEN

Sheet 3

- Don't hope I offend any of the Nigerians here today

<u>419 Scam</u>

- Maybe the most well known cybercrime
- Spanish prisoner scam dating back to late 19th Century
  - Con man tells victim he is a wealthy person imprisoned in Spain
  - Victim raised money for his release but down the road difficulties arise so more money is raised and it goes on and on.
- Based on trust/confidence and greed
- E-mails promising a lot of money, but only some help is needed.
- Advanced payment is necessary
- Google translate is used!
- In 2006 61% was traced back to US, and only 6% to Nigeria.
  - Netherlands and Spain also very well known to house a lot of fraudsters
- Very complex. A lot of phones, a lot of identities for the fraudsters
- Always wonder why people fall for it
  - Why are the victims often in the US?
  - 7 lawyers from the IBA got scammed by the taxi driver, without much complaining
  - Apparently we feel comfortable in being scammed.

<u>Skimming</u>

- Also well known, uses technology to copy ATM card when inserted in the ATM.
- Security code usually seen with a camera
- Banks can see if a card is skimmed because every transaction, one of the two control numbers change on your card.
- If the numbers don't add up anymore, the bank can see a card is skimmed
- How do I know: a client argued he was skimmed, but the bank proved to my disappointment he was not

<u>Phishing</u>

- E-mails asking you to go to website and fill in your security code.
- Fake websites which look like banks.
- Criminals are getting smarter

- Now I receive phishing e-mails warning me for phishing e-mails
    - But to fight phishing, the bank needs my details again.

Spamming

- Lots and lots of offers for Viagra every day
- Illegal in a lot of countries, but difficult to prosecute
- Millions and millions are made, not only by fraudsters, but also by people selling spam filters.
- Spamhouse, organization against spam, uses blacklists to fight spam
- Usually botnets are used

Hacking

- Very broad definition
- A lot of different categories
- We all know anonymous
- Difference between ethical hacking, and non-ethical hacking.
    - Thin line between this
- Hacking used to commit other cybercrime like creating botnets
    - Spamming
    - Stealing of digital property.

Grooming

- Big issue in the Netherland
- People chatting with minors to try and date them and abuse them
- get them to do things before their webcam

Child pornography

- High priority everywhere
- US lawyers tell me these cases are the worst: guaranteed years in jail
- the Netherlands recently introduced minimum sentence jail time for child pornography
- Hot topic in the Netherlands is digital child pornography

Sheet 4

- Introduce the cybercrime spectrum by mentioning a few cases

Keizersgracht 332
1016 EZ Amsterdam
T +31 (0)20 627 5411
F +31 (0)20 622 6577
E info@deroosenpen.nl
I www.deroosenpen.nl

DE ROOS & PEN

Case of Robert M.

- Biggest case of child pornography in the Netherlands
- World wide network
- Started with child pornography picture of a boy with a toy miffy in his hand
- FBI thought it was a Dutch kid
- Picture shown on Dutch tv and Robert M. was arrested

Sheet 5

- Lot of discussion on the fact that his picture was shown after arrest
- Very intelligent security. Police couldn't crack his codes.
- TrueCrypt was used, build also partly by Assange to protect whistleblowers and others
- Robert M used 30 digit passwords.
- It would have taken 6000 years to crack the code.
- Eventually he gave the passwords voluntarily
- Cooperation not reflected in sentence
- TBS: Compulsory treatment psychiatric hospital (no end date)

Sheet 6

- We all know the mega upload case
- As you can see, Kim Dotcom did well for himself.
- There are probably people in the audience who know the case much better than I do
- Watch out what I say
- Biggest file hoster in the world
- Kim Dotcom and Dutch programmer Bram van der Kolk suspects
- Estimated harm $500 million dollars
- 630 servers confiscated in Canada, US and the Netherlands
- Reaction from Anonymous with DDos attacks
    - Just plain revenge it seemed
- Illegal searches in New Zealand. Much litigation
- Kim Dotcom is thinking of a political career?
- Fighting extradition, unknown if he will ever be extradited to the US

Keizersgracht 332
1016 EZ Amsterdam
T +31 (0)20 627 5411
F +31 (0)20 622 6577
E info@deroosenpen.nl
I www.deroosenpen.nl

DE ROOS & PEN

Sheet 7

- One of the biggest organization combating Spam
- IP Blacklist
- Target for hackers and people commiting cybercrime
- March 2013 attack by Dutch citizen (based in Spain), Sven K. from Cyberbunker
- Biggest attack ever
- DDos attack using Botnet
- Slowed down internet all over the world
    - So many infected computers were used
    - A lot of websites were unavailable.
- Sven K. was extradited to the Netherlands.
- In the UK another suspect was arrested

Sheet 8

- Most used way of committing cybercrime is by using botnets
- Network of infected computers (zombies)
    - Infect them through Trojans etc.
- One command and control center
- Cyberattacks
- DDos (distributed denial of service)
    - Making all the computers in your Botnet trying to reach a website at one
    - So many requests are made the website goes offline
- Monetize botnet
    - Use it to send Spam
    - Adwords fraud
        - We all know competitor clickfraude
        - Your competitor keeps on clicking on your adwords which costs you money
        - Google has systems preventing this
        - Is u put Adwords on your own site
        - You get money from Google for every click through your site
        - If you use a botnet to do the clicking for you, you earn money
    - Click hijacking
        - Send infected computers to other sites
        - If you search for Itunes, it sends you to a site which has nothing to do with Apple

- Advertising replacement
  - Controller of botnet replaces adds
  - He gets money from companies he places the adds for.

Sheet 9

- Netherlands relevant internet hub
  - Good infrastructure
    - Amsterdam Internet Exchange number 2 in Europe (after Germany)
    - 1400 Gigabytes per second
    - Lot of discussion recently when Exchange told they were setting up shop in US
    - Privacy/Prism issues
  - Time zone
  - First country in the EU with net neutrality law
    - prohibits internet providers from interfering with the traffic of their users.
- Problems
- Law not up-to-date
  - Lot of criticism
  - Difficult to change the law
  - Draft law on cybercrime in 2010, recently a new one drafted because there was so much criticism.
- Complex crime
  - Worldwide
  - Jurisdictional issues
    - Encryption orders to providers in other jurisdictions not possible
    - Where is the crime committed?
      - Dutch jurisprudence: In The Netherlands if there is a connection with the Netherlands, or aimed at Netherlands
    - Investigation cross border
      - Cybercrime treaty
        - Allowed to seize Public information in other countries
        - Network search in other country with permission (third) party who has access to it
        - Only for existing data, not for streaming data

Keizersgracht 332
1016 EZ Amsterdam
T +31 (0)20 627 5411
F +31 (0)20 622 6577
E info@deroosenpen.nl
I www.deroosenpen.nl

- Smart suspects
- Less intelligent police
  - High Tech Crime Team
  - Cooperation with private parties:
    - National Cyber Security Center
    - Computer Emergency Response Team

Sheet 10

- Content removal order
  - Immunity for hosting providers
  - European E-commerce directive
  - Difference between civil and criminal protection
  - Definition of knowledge
- Goods vs. data
  - Definition of goods.
  - In general: data does not qualify as goods, so you cannot steal data
  - Under very specific circumstances data can qualify as 'goods'
    - Runescape amulet, worth money, you can lose possession
  - New criminal offence: possession of illegally obtained data
    - Illegally obtained: Hacking
    - Theft of confidential files by employee
  - Ethical publication stolen data
    - Public interest?
    - Journalists, whistleblowers. ethical hacking!
    - Use of government of stolen data? CD's with Swiss bank accounts.

Sheet 11

- Hacking by police
  - Authorization judge
  - Plant software (using webcam, microphones)
  - Check data, remove data
  - Network search vs. cloud search
  - Even possible in servers in other jurisdictions
    - Belgium, France, Germany have similar laws

Keizersgracht 332
1016 EZ Amsterdam
T +31 (0)20 627 5411
F +31 (0)20 622 6577
E info@deroosenpen.nl
I www.deroosenpen.nl

- Belgium: Network search (also outside jurisdiction), but no hacking
- Germany: Hacking only for terrorism, much discussion about lawfulness
- France : possibility of installing device to gain access to data

- Draft seems in breach with international treaties on jurisdiction.
- Difference between stored data and streaming data

- Even possible in computers of third parties
  - For example infected zombie computers
- Privilege issues? Police snooping around your data without you knowing!
- Hacking smartphone (checking locations)

- Decryption order against defendant
  - Terrorism
  - Child pornography
  - Apparently Terrorism and Child pornography can be put on the same level?
  - 3 years imprisonment
  - Protection against self incrimination?
    - France, England has similar law, English court of appeal ruled it was not in breach of the right of protection against self incrimination
    - US also had decryption order, in breach of 5th amendment rights?
      - (United States vs Fricosu) Government gave Fricosu immunity precluding it from "using her act of producing the unencrypted contents of the laptop computer against her". How far does that immunity go?
      - Boucher 2009, decryption order given
      - Feldman: no decryption, in breach of 5th amendment rights

Sheet 12

- Framework decision EU on attacks against information systems
- Improve cooperation
- Gaps and differences in Member States
  - Common approach
  - Common definitions
- Introduction of ethical hacking?
  - White hat hackers

Keizersgracht 332
1016 EZ Amsterdam
T +31 (0)20 627 5411
F +31 (0)20 622 6577
E info@deroosenpen.nl
I www.deroosenpen.nl

DE ROOS
& PEN

Niels van der Laan

Partner at De Roos & Pen, The Netherlands, Amsterdam

CRIMINAL
DEFENCE
LAWYERS

DE ROOS & PEN

Old School ATM Heist

DE ROOS & PEN

New School ATM Heist

Cyber-attacks behind possibly record-breaking bank heist

comments Like 282 Tweet 68 +1 4 Share 7 More +

DE ROOS & PEN

Cybercrime

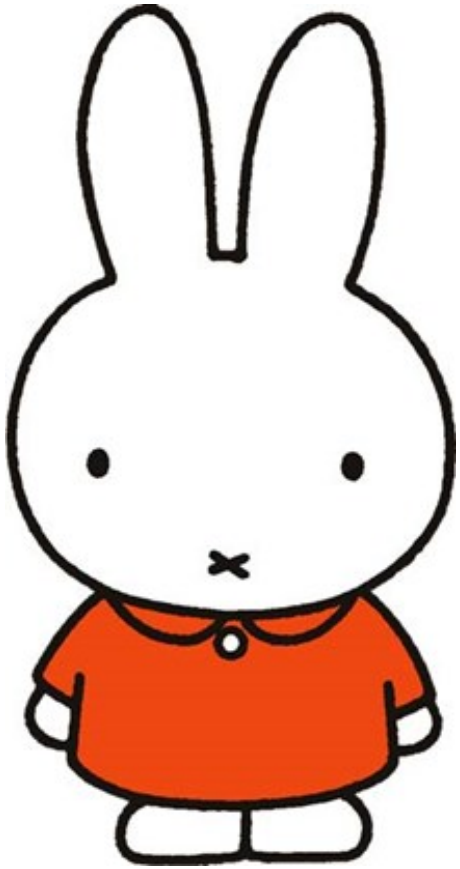
- 419 fraud
- Skimming
- Phishing
- Spamming
- Hacking
- Grooming
- Child Pornography
- Etc…

CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Case of Robert M.

- Biggest Child pornography case ever
- World wide network
  - USA
- Started with picture of Dutch kid with Miffy (Nijntje)
- Research to the kid
- Resulted in arrest of Robert M.



CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Case of Robert M.

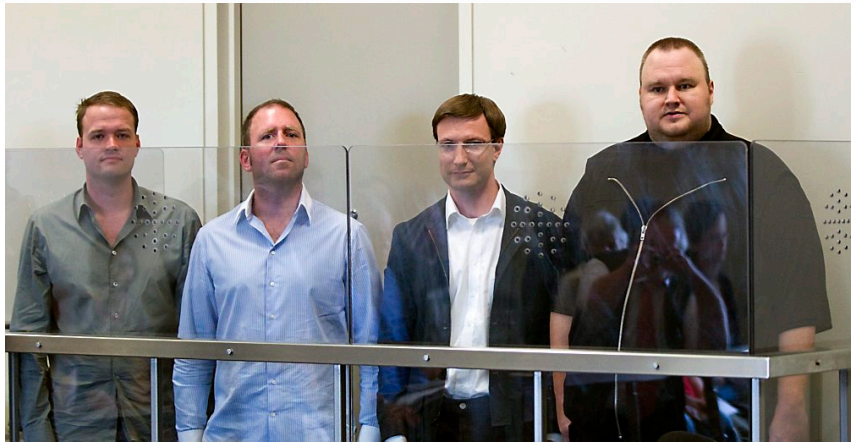
- Picture of suspect shown on national TV (after arrest)
- Layers of encryption, TrueCrypt
- Cooperation suspect
- Abuse of 83 kids
- 46.803 pictures, 3672 movies
- 19 years and TBS

CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Mega Upload

- Biggest file hoster in the world
- Kim Dotcom and Dutch programmer Bram van der Kolk suspects
- Estimated harm $500 million
- 630 servers confiscated in Canada, US and the Netherlands
- Reaction from Anonymous with DDos attacks
- Illegal searches
- Political career?
- Extradition?



CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Spamhouse

- Organization combating Spam
- IP Blacklist
- Target for hackers
- March 2013 attack by Dutch citizen (based in Spain), Sven K. from Cyberbunker
  - Biggest attack ever
  - Slowed down internet all over the world
- DDos attack using Botnet

CRIMINAL DEFENCE LAWYERS

Mirror NEWS

Real news, real entertai

FRONT PAGE | NEWS | SPORT | 3AM | TV | LIFESTYLE | MONEY | PL

News › World news › Crime

By Damien Fletcher | 5 Comments | 28 Mar 2013 07:56

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world

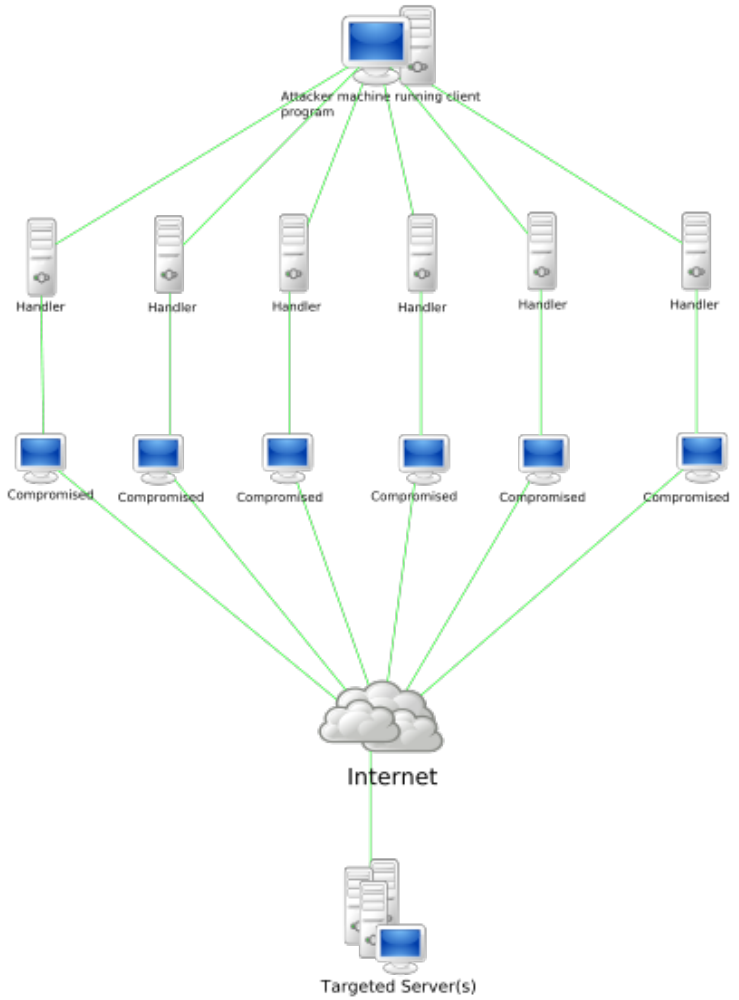
A row between an anti-spam group and a web-hosting company sparked retaliation attacks affecting the wider internet.

Tweet 41 Like 89 Send

DE ROOS & PEN

Botnets

- Network of infected computers (zombies)
- One command and control center
- Cyberattacks
  - DDos (distributed denial of service)
- Monetize botnet
  - Spam
  - Adwords fraud
  - Click hijacking
  - Advertising replacement



CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Cybercrime in the Netherlands

- Netherlands relevant internet hub
  - Good infrastructure
  - Time zone
- Problems
  - Law not up-to-date
  - Complex crime
  - Worldwide
    - Jurisdictional issues
  - Smart suspects
  - Need for intelligent investigators
    - High Tech Crime Team
    - Cooperation with private parties

CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Proposed law against cybercrime

- Content removal order
  - EU E-commerce directive
  - Immunity for hosting providers
    - Civil vs. criminal protection
- Goods vs. data
  - Possession of illegally obtained data
  - Ethical publication stolen data
    - Whistleblowers protection

CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

Proposed law against cybercrime

- Hacking by police
  - Plant software, check data, remove data
  - Network vs. Cloudsearch
  - Jurisdictional issues
- Decryption order against suspect
  - Terrorism and child pornography
  - Protection against self incrimination
    - France, UK have similar laws
    - Discussion in United States (Fricosu, Boucher, Feldman)

CRIMINAL DEFENCE LAWYERS

DE ROOS & PEN

European Union

- Framework decision EU on attacks against information systems
- Improve cooperation
- Gaps and differences in Member States
  - Common approach
  - Common definitions
- Introduction of ethical hacking?
  - White hat hackers

CRIMINAL DEFENCE LAWYERS