Regional Conference on Policies and Strategies on cybercrime for the Caribbean Community

The role of the private sector

Santo Domingo – 13 June 2019

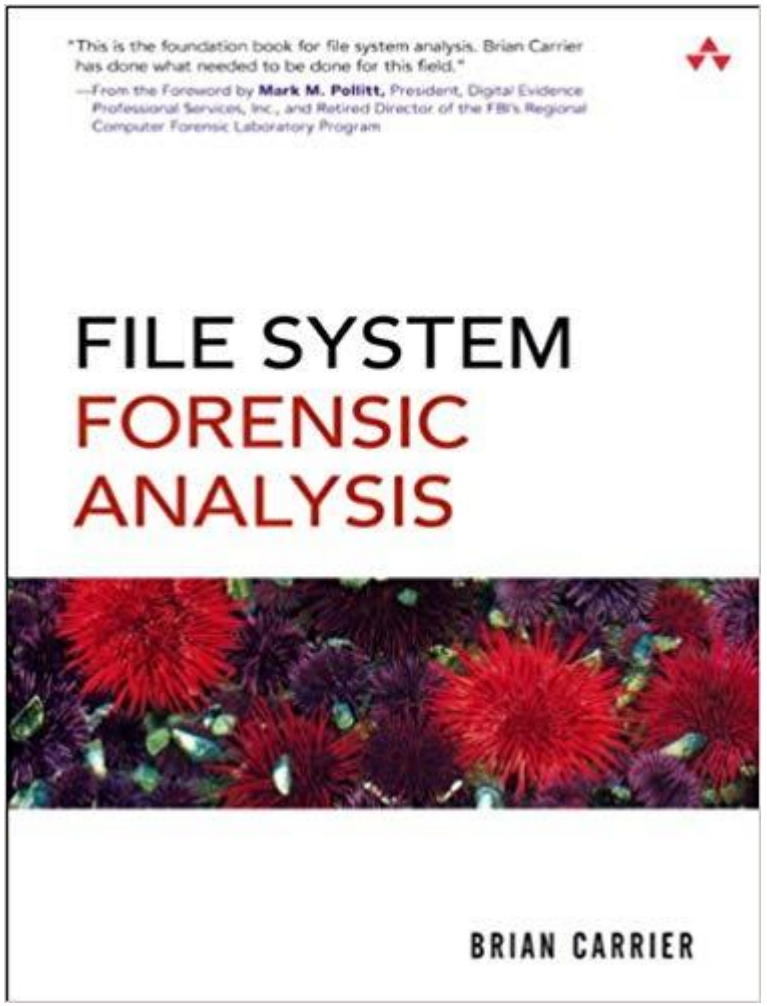
Sources of evidence

- Internet Service Providers are holders of potential evidence such as:
  - Subscriber information
  - Traffic data
  - Content data
- Data preservation
- Online services are numerous today, way beyond email and social networks. As good as all online service maintain transaction logs. Request made to Uber is increasingly common.

Forensics knowledge

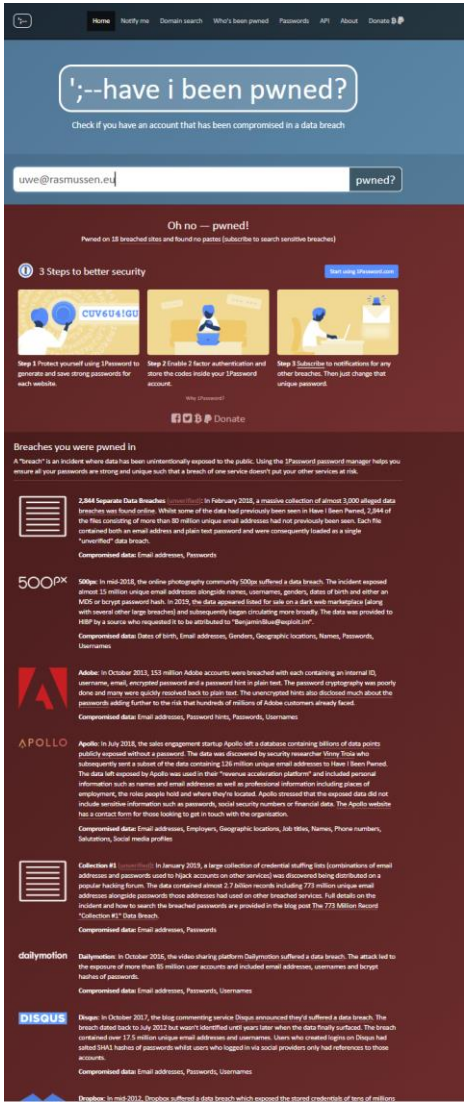
Technology companies can explain the innards of their products such as:

- The file system
- Log files kept by the operating system or applications
- IMEI numbers and what they say about device models
- Authentication reliability information
- Memory/RAM forensics



Victims of cybercrime

- Companies have frequently been reluctant to report cybercrime incidents.
- Various legislation have introduced mandatory breach notifications such as:
  - HIPAA
  - Network and Information Security Directive
  - GDPR

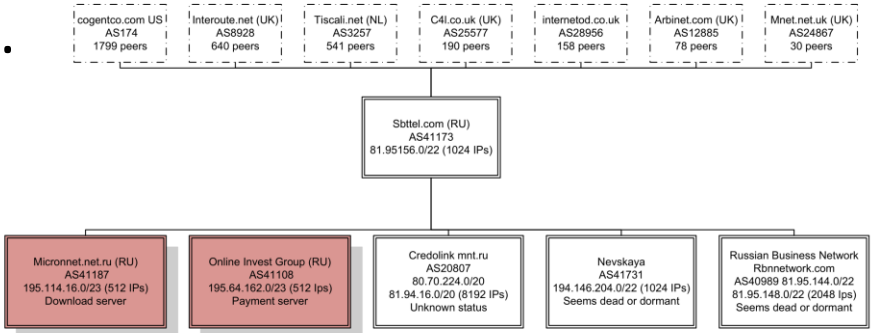


Witnesses to crime

- The private sector may have collected information on cybercrime for different reasons:
  - Microsoft Tech Support Scams
  - TeliaSonera database of communications to unallocated IP addresses
- Similarly CERTs, such as financial sector CERTs could provide information about unlawful activity they see; including recurring phishing or hacking attempts.

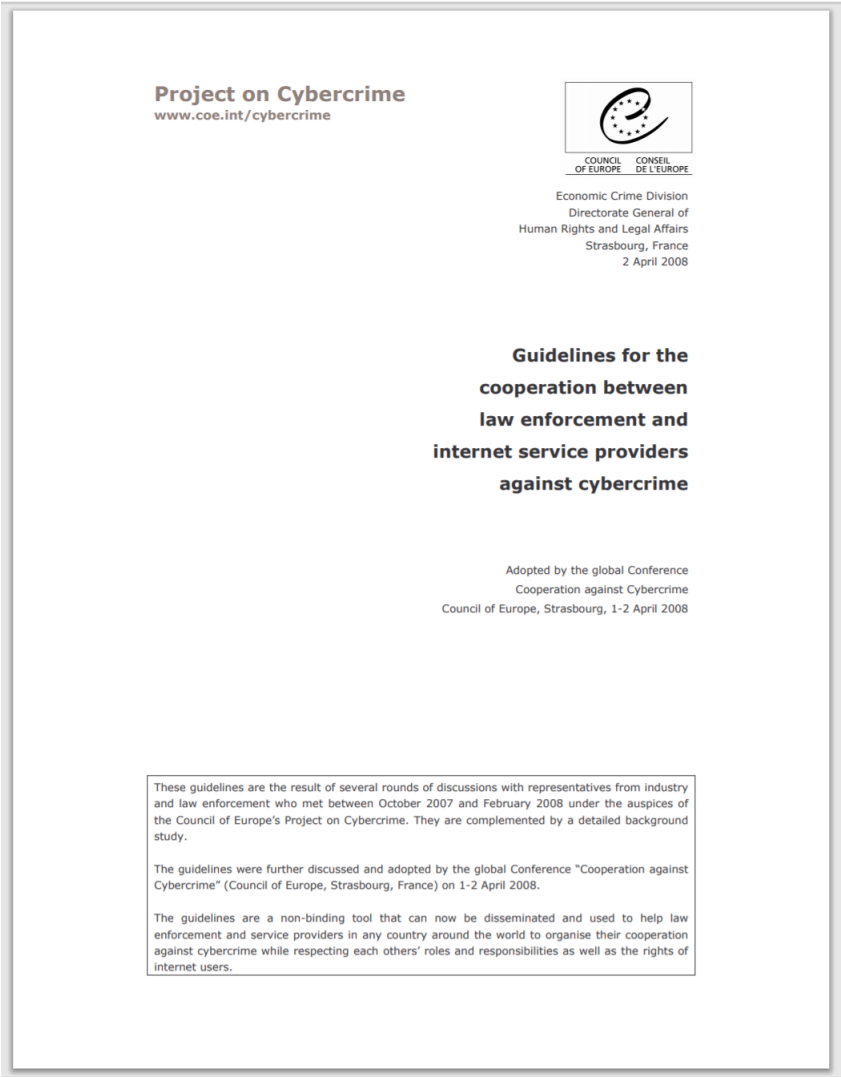
Improving policies and practices

- Conversations with the private sector about detected cybercrime can help them adopt policies or codes of conduct that would eliminate it.
- ICANN had a policy for the fair distribution of IP addresses but needed to adopt a policy for revoking IP addresses.
- Providing free domain names lead to an increase of Advance Fee Fraud from the provider. Having a policy requiring some identification through payment systems reduced this.



Forums with the private sector

- Often the private sector is happy to participate in forums to discuss cybercrime in all its facets: whether it is as a victim, witness, or general discussions on cybercrime.
- The Council of Europe has published guidelines on cooperation between LE and ISPs on cybercrime which could be used to improve cooperation.



Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France
2 April 2008

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted by the global Conference
Cooperation against Cybercrime
Council of Europe, Strasbourg, 1-2 April 2008

These guidelines are the result of several rounds of discussions with representatives from industry and law enforcement who met between October 2007 and February 2008 under the auspices of the Council of Europe's Project on Cybercrime. They are complemented by a detailed background study.

The guidelines were further discussed and adopted by the global Conference "Cooperation against Cybercrime" (Council of Europe, Strasbourg, France) on 1-2 April 2008.

The guidelines are a non-binding tool that can now be disseminated and used to help law enforcement and service providers in any country around the world to organise their cooperation against cybercrime while respecting each others' roles and responsibilities as well as the rights of internet users.

Questions