

# **Spot *Spam***

## **The European Spambot Project**

**Przemek Jaroszewski**  
**CERT Polska/NASK**

**18th TF-CSIRT Meeting, Vilnius, Lithuania**  
**25-26th May 2006**

- eco.de - The Association of German Internet Enterprises maintains a hotline to deal with complaints about illegal and offensive internet content

Many illegal content reports handled by the hotline involve spam.

eco was contacted by Microsoft to assist with spam cases originating from MS Hotmail accounts, gathering evidence for court trials.

Why just focus on one provider? This idea may work universally.

- **NASK operates CERT Polska, which handles spam cases and has technical expertise in analyzing and tracing this kind of messages**
- **EU approved the project and provided funding within the Safer Internet Programme. Additional funding is provided by Microsoft.**

## **Sending spam is illegal in some jurisdictions under certain conditions.**

The following areas are a particular concern:

- spam mails which contain harmful or illegal content or refer users to such content, e.g. indecent pictures or child abusive pictures,
- inappropriate e-mail communication which is sent to children and young people, e.g. pornographic pictures contained in spam mails,
- fraudulent emails promoting products and services regulated by law (drugs, financial services), or try to steal personal data from unsuspecting users ("phishing")

## SpotSpam is aiming to address the following problems:

- **technical tricks** commonly used by professional spammers make it difficult for an average user to identify the actual offender
- **international dimension** of most spam cases
- **lack of single point of reporting** in most cases makes users confused and not willing to take any actions
- **taking legal action from individual cases** is ineffective and results with penalties that do not repel spammers

## Modules Overview

- Module A: Preparatory Research
- Module B: Memorandum of understanding on how to gather evidence
- Module C: Memorandum of understanding on how to share evidence
- Module D: Definition and implementation of a prototype database

## Module A: Preparatory Research

When it comes to drafting policy papers on border-crossing action and common approaches, it has to be ensured that:

- the legal and factual circumstances in at the national level are known, such as the schedule of responsibilities between private and public bodies in the fight against spam,
- existing mechanisms and procedures are known and analysed to ensure compatibility with the approaches to be developed,
- the legal restrictions are known to make sure that the approaches to be defined do not violate national law

## Module B: MoU on how to gather evidence

It is necessary to enter into agreements with appropriate (read: capable of taking actions) organisations on how to collect evidence on spam cases. These organisations include:

- hotlines taking complaints about Internet content or services from the public
- Internet Service Providers' abuse departments or IRTs
- governmental reporting points
- consumer protection agencies

## Module C: MoU on how to share evidence

Ways to use the evidence can include and not be limited to:

- try to identify the origin of spam or the spammer and then take action against the spammer
- try to contact owners and administrators of the infrastructure used to transmit spam in order to fix the problems technically and/or administratively
- responding to requests from third parties which intend to take action against spammers, whether similar cases have been reported, so that joint action can be facilitated
- searching the database for terms usually found in connection with illegal content so that those items can be reported to an appropriate national hotline or law enforcement authority
- providing information to blacklisting services

Thus, a memorandum of understanding is required on what information shall be shared, with whom and under what conditions.

## Module D: Definition and implementation of a prototype database

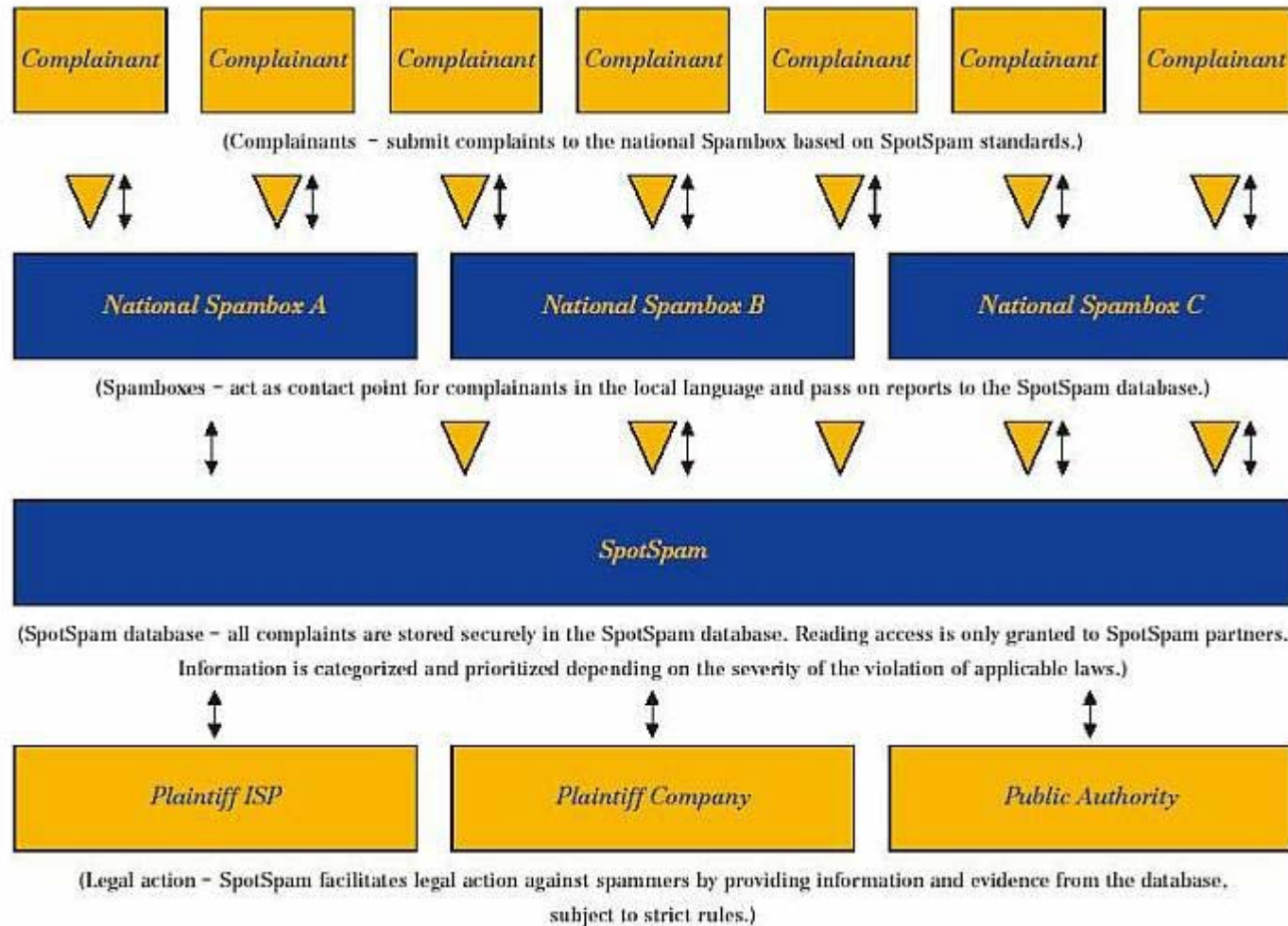
The technical development is split into several parts:

- development of a searchable spam database,
- development of a tool to categorise reports / notification mechanism,
- development of a tracing tools / feasibility study,
- specification of technical requirements for operations after a public launch

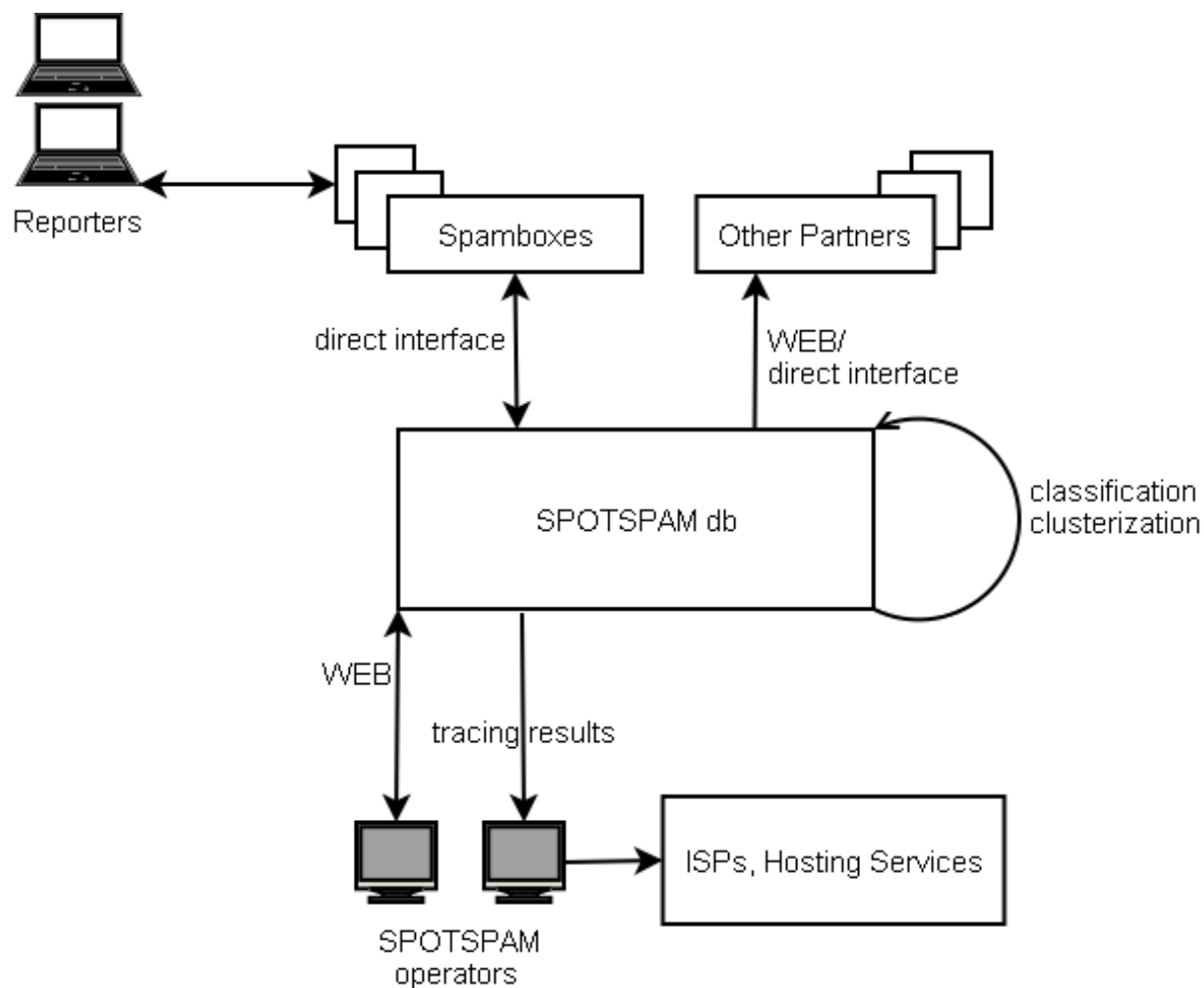
One of the critical tasks for the database is to be able to identify spam campaigns by clustering identical/similar messages that potentially originate from the same source.

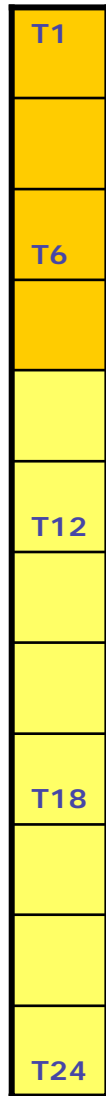
Obviously, it must be also capable of running queries defined by memoranda of understanding.

# SpotSpam – overview diagram



# SpotSpam – information flow diagram





**Sep 05: Project started**

T1

**Mar 06: Specification of the database and auxiliary tools (completed)**

T6

**May 06: Research Report (due)**

**Jul 06: 1<sup>st</sup> draft of memoranda od understanding**

T12

**Sep 06: Preliminary prototype database impementation**

T18

**Apr 07: Final prototype database impementation**

**Jun 07: Final drafts of memoranda of understanding**

T24

**Sep 07: Technical requirements for operation after public launch**

## Foreseen problems

- **information gathering**

- certain formats are required, full headers and attachments
- how to protect database against *false positives*?
- memoranda of understanding must be covering
  - privacy protection
  - personal data protection

- **technical problems**

- spam proves to be hard to analyze – both headers and content of the message are scrambled by spammers to bypass blacklists and spam filters

- **usage of evidence**

- regulations vary even within EU
  - in Poland, only unsolicited commercial e-mail is considered spam and must be reported by the recipient
  - in the UK, doctrine of precedent can be applied
- from user's point view „fire and forget” behaviour is desired



**SpotSpam is a 24 month contract under the EC's Safer Internet Programme.**

- partners: eco (DE), NASK (PL)
- support: Microsoft
- cooperation: MessageLabs, Spamhaus.org, SignalSpam

**<http://www.spotspam.net/>  
[mail@spotspam.net](mailto:mail@spotspam.net)**

# Thank you!

For information giving and receiving:

- [przemek@cert.pl](mailto:przemek@cert.pl)
- [mail@spotspam.net](mailto:mail@spotspam.net)