Update on SPOTSPAM project activities

Przemek Jaroszewski
CERT Polska / NASK
przemek@cert.pl

21\textsuperscript{st} TF-CSIRT meeting
Prague, 3\textsuperscript{rd} of May 2007
What is SpotSpam?

- SPOTSPAM is a EU project under EC’s Safer Internet Programme
- Consortium: eco (Association of German Internet Providers) & NASK
- Support: Microsoft
- Goals of the project: prepare legal and technical basis for gathering and sharing evidence against spammers
- Timeline: September 05 – September 07
What is SpotSpam?

- **Complainant**
  - Complainants submit complaints to the national Spambox based on SpotSpam standards.

- **National Spambox A**, **National Spambox B**, **National Spambox C**
  - Spamboxes act as contact points for complainants in the local language and pass on reports to the SpotSpam database.

- **SpotSpam**
  - All complaints are stored securely in the SpotSpam database. Reading access is only granted to SpotSpam partners. Information is categorized and prioritized depending on the severity of the violation of applicable laws.

- **Plaintiff ISP**, **Plaintiff Company**, **Public Authority**
  - Legal action - SpotSpam facilitates legal action against spammers by providing information and evidence from the database, subject to strict rules.
What is the plan?

- Spambox operators sign an agreement with SpotSpam
- Complainants register with their local Spambox. They must agree to submit signed evidence in case a court case is launched. They must also certify that all reports submitted by them will actually be spam.
- Complainants can send reports via a web form, email forward, and hopefully with a mail client plugin. Dedicated means for bulk submissions will be evaluated.
- The reports are stored in central database, which can be queried against IP ranges, email addresses, message subjects etc. Only some indicative data is returned (eg. how many reports are found to match given criteria)
- Interested parties can request full data upon identification if these are required to launch a court case
What is the plan?

- Some additional fireworks and special effects:
  - Identification of spam campaigns → more complex picture than just looking at individual messages
  - Snapshots of spamadvertised will be taken automatically upon submission to preserve evidence
  - DNS changes will be tracked
  - Information about abused hosts, spamadvertised URLs, targeted domains
  - Input from spamtraps can be considered a pretty good evidence of unsolicited communication
What is done so far?

- eco investigated potential legal problems with a positive outcome: data can be collected and shared within EU and countries of equivalent data protection level (e.g., Canada, Switzerland)
- Set of standard documents (contracts, data request forms, authentication sheets) was prepared for parties willing to share and request information
- NASK prepared a prototype of application to collect and analyze spam reports
What is still to be done?

- Agree with partners on the technical means of data (some already have their databases, some don’t care at all)
- Agree with partners on what types of database queries would give them most useful information for their kind of activities (ISP, regulatory body, trademark owner)
- Choose a working business model
- Develop elaborate and sophisticated methods for clustering and categorising of messages 😊
More information can be obtained from:

- http://www.spotspam.net/
- mail@spotspam.net
- myself in person or by email: przemek@cert.pl
CERT POLSKA

zgłaszanie incydentów: cert@cert.pl
strona internetowa: www.cert.pl
tel. +48 (22) 523 12 74
fax. +48 (22) 523 13 99
adres pocztowy:
NASK - CERT Polska
ul. Wąwozowa 18
02-786 Warszawa
Polska

DZIĘKUJEMY ZA UWAGĘ