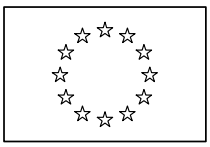

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 15.11.2006
COM(2006) 688 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

On Fighting spam, spyware and malicious software

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

On Fighting spam, spyware and malicious software

(Text with EEA relevance)

1. PURPOSE OF THE COMMUNICATION

Society is becoming more and more aware of how essential modern electronic communications networks and services are for everyday life, in business or at home. A wide take-up of services depends on trustworthy, secure and reliable technologies. The Commission Communication on a Strategy for a secure Information Society[1] aims at improving the security of network and information at large and invites the private sector to address vulnerabilities in network and information systems that can be exploited to spread spam and malicious software. The Commission Communication on the Review of the EU Regulatory Framework proposes new rules to strengthen security and privacy in the electronic communications sector[2].

The present Communication deals with the evolution of spam[3], and threats such as spyware and malicious software. It takes stock of efforts made so far to fight these threats and identifies further actions that can be taken, including:

- strengthening Community law

- law enforcement

- cooperation within and between Member States

- political and economic dialogue with third countries

- industry initiatives

- R&D activities.

---

1 COM(2006) 251 final
2 COM(2006) 334 final.
3 COM(2004) 28 final

2. THE PROBLEM - THE EVOLVING NATURE OF THREATS

Spam[4] has grown significantly over the last 5 years[5]. Industry sources report that spam now accounts for 50-80% of messages addressed to end-users.[6] Although the biggest portion of spam originates from outside the EU, European countries now account for 25% of relayed spam messages[7]. The worldwide cost of spam has been estimated at €39 billion in 2005. Spam costs to major European economies have been estimated to be around respectively €3,5 billion – Germany, €1,9 billion –United Kingdom and €1,4 billion - France[8]. Spamming is considered a 'business' of its own. Spammers rent or sell lists of harvested e-mail addresses to companies for marketing purposes. Spam over the internet is especially lucrative. This has to do with the reach of the medium and the low costs involved in sending massive amounts of messages. At the same time moderate investments to fight spam can also deliver significant results. As an example, in the Netherlands an 85% reduction in Dutch spam was achieved by investing **€570 000** in equipment to fight spam.

From a mere nuisance unsolicited e-mail has become increasingly fraudulent and criminal in nature. A prominent example is the use of phishing e-mails that lure end users into giving up sensitive data via imitation websites purporting to represent genuine companies, raising concerns about possible identity fraud and damage to companies' reputations. The dissemination of spyware by e-mail or through software to track and report a user's on-line behaviour continues to increase. Spyware may also collect personal information such as passwords and credit card numbers.

The sending of massive amounts of unsolicited e-mail is greatly facilitated by the spread of malicious codes such as worms and viruses. Once installed, they allow an attacker to take over control of an infected computer system and turn it into a 'botnet',[9] hiding the identity of the real spammer. Botnets are hired by spammers, phishers, and spyware vendors for fraudulent and criminal purposes. Industry experts estimate that 'botnets' relay over 50 percent of abusive e-mails [10]. The spread of spyware and other types of malicious codes attacking consumers and businesses has a considerable economic impact. The global financial impact of malware has been estimated about €11 billion in 2005[11].

3. THE WORK DONE SO FAR - ACTIONS UNDERTAKEN SINCE 2004

The EU adopted in 2002 a **Directive on Privacy and Electronic Communications** that puts a **ban on spam**[12] by introducing the principle of consent-based marketing to natural persons. In January 2004, the Commission presented a Communication on spam identifying actions to

---

4 Spam refers to sending unsolicited communications –e.g. by e-mail- for commercial purposes. However, unsolicited e-mail messages may also carry malicious software and spyware.

5 In 2001 spam was 7% of global e-mail traffic.

6 Symantec 54%; Messagelabs 68,6 MAAWG 80-85.

7 Q1 2006 (Sophos) Asia 42.8%, N. America 25.6, Europe 25.0, S. America, 5.1, Australasia 0.8 Africa 0.6, Other 0.1.

8 Ferris research, 2005.

9 Botnets are compromised computers used by spammers to send bulk e-mails by installing hidden software that turns computers into mail servers without the users' knowledge.

10 Symantec top botnet infected countries, (Q 3-4 2005) : US 26 %, U K 22%, China 9%, France, S. Korea, Canada 4%, Taiwan, Spain, Germany 3%,Japan 2%.

11 Computer Economics: the 2005 Malware Report.

12 Art. 13 Directive 2002/58.

complement the Directive[13]. The Communication stressed the need for action by various actors in the areas of awareness, self-regulation/technical actions, cooperation and enforcement. The Commission has started to include the issue of the fight against spam, spyware and malware in its dialogue with third countries. In addition, the Unfair Commercial Practices Directive[14] protects consumers against aggressive commercial practices; cross border cooperation to fight such practices comes under the Regulation on Consumer Protection Cooperation[15].

3.1. Awareness actions

The Commission Communication contributed in raising awareness of spam at national and international level around the globe. At EU level, the **Safer Internet *plus* programme** promotes safer use of the Internet and new online technologies, particularly for children, as part of a coherent approach by the European Union.

Member States have launched or supported **campaigns** to make users aware of the spam problem and how to deal with it. Generally ISPs have taken responsibility in providing their customers with advice and assistance on how to protect themselves against spyware and viruses. The Commission hosted an OECD **workshop** on spam in February 2004. The Commission also contributed actively to the OECD **Anti-Spam Toolkit** that provides a comprehensive package of regulatory approaches, technical solutions, and industry initiatives to fight spam.

The UN World Summit on the Information Society[16] **recognised** that spam should be dealt with at appropriate national and international levels. WSIS thematic conferences have been held by the ITU in 2004 and 2005. The WSIS Tunis Agenda adopted in November 2005 calls to deal effectively with the significant and growing problem posed by spam[17].

3.2. International Cooperation

Spam is a cross-border issue, and several cooperation initiatives and cross-border enforcement mechanisms have been put in place. The Commission has set up a **Contact Network of Spam Authorities** (CNSA), which meets regularly, exchanges best practices and cooperates on enforcement across borders. The CNSA has drawn up a cooperation procedure[18] to facilitate cross-border handling of spam complaints. The Commission services support and participate as observers in the **London Action Plan**, which gathers enforcement authorities from 20 countries and has also adopted a cross border cooperation procedure. A joint EU CNSA – LAP workshop was held in November 2005. The **OECD** adopted a Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam which was adopted in April 2006, urging enforcement authorities to share information and work together[19].

---

13 *Supra* 3.

14 Annex 1, point 26, Directive 2005/29/EC

15 Regulation (EC) 2006/2004

16 WSIS, Geneva, December 2003.

17 Tunis Agenda, para. 41.

18 http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf

19 http://www.oecd-antispam.org/

The Commission is further promoting **international cooperation initiatives**. The US and the EU have agreed 'to cooperate to tackle spam through joint enforcement initiatives, and explore ways to fight against illegal "spyware" and "malware". The Commission also takes part in the Canadian International Collaboration working group on Spam. Discussions are taking place with major international partners e.g., China, Japan. Concerning Asia the Commission initiated a Joint Statement on International Anti-spam Cooperation which was adopted at the ASEM conference on eCommerce in February 2005[20].

The Tunis Agenda, adopted by the World Summit of Information Society in November 2005, stresses that internet security is an area where a better international cooperation is needed and that this issue will need to be addressed in the framework of the enhanced cooperation model for internet governance that will be implemented as a follow-up of the Summit.[21].

3.3. Research and Technology development

Under the 6th RTD Framework Program, the Commission has launched projects to help stakeholders fight spam and other forms of malware. These projects[22] range from general network monitoring and detection of attacks to the specific development of technologies to build filters to detect spam, phishing and malware. Achievements include the establishment of a research community dedicated to malware containment and the development of a European infrastructure to monitor Internet traffic. Recently-started activities concern adaptive phishing filters which can detect unknown threats, and cyber attacks. The financial effort dedicated to these activities amounts to €13.5 million.

3.4. Industry actions

The Commission welcomes industry's pro-active role in relation to spam. Service providers in general have taken **technical measures** to tackle spam, including better spam filters. ISPs have set up **help desk support** and provide users with software against spam, spyware and malware. Many ISPs have **contractual clauses** in place that forbid on-line malpractices. In a recent civil UK court case a €68 800 fine was imposed on a spammer for breach of contract. Industry groups have adopted best practices to prevent on-line phishing and to improve filtering methods[23].

Mobile operators have acted Industry codes of conduct foresee taking action against unsolicited messages. The GMSA has published a Code of practice on Mobile spam in 2006. Currently the Commission co-funds the Spotspam initiative – a partnership between private and public bodies which aims to build a database to facilitate the cross border investigation and enforcement of spam cases[24].

---

20 http://www.asemec-london.org/

21 Tunis Agenda para's 39-47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

22 www.diademhttp://cordis.europa.eu/fp6/projects.htm#search

23 http://www.maawg.org/home/

24 http://www.spotspam.net

3.5. Enforcement actions

It is clear that taking up the fight against spam delivers results. Filtering measures imposed in Finland reduced the proportion of spam in the transmitted e-mail from 80 % to about 30 %. A large number of authorities have undertaken enforcement efforts to stop spammers[25].

There are however significant differences between Member States in the actual number of prosecuted cases. Some authorities have launched a hundred or more investigations that have led to successfully ending and penalising spam activities. In other Member States the number of cases investigated has not been more than a handful or in some cases zero.

Most actions have been targeted at **'traditional' forms** of spam; **other noted threats have hardly been prosecuted** even though they create major risks.

4. THE WAY FORWARD: WORK TO BE DONE

4.1. Action at Member States level

This section covers actions targeted at Governments and national authorities in particular related to enforcement and cooperation.

4.1.1. Critical success factors

The persistency and evolving nature of the problem calls for greater involvement and prioritisation by Member States. Actions should in particular address 'professional' spammers, phishers and the spreading of spyware and malware. Critical success factors are:

– A strong commitment by central government to fight on-line malpractices

– Clear organisational responsibility for enforcement activities

– Adequate resources for the enforcement authority.

Currently, these factors are not present in all Member States.

4.1.2. Coordination and integration at national level

Under the e-Privacy Directive and the General Data Protection Directive[26], national authorities have the power to act against the following illegal practices:

- sending unsolicited communications (**spam**)[27]**;**

- unlawful access to terminal equipment; either to store information -such as **adware** and **spyware** programs- or to access information stored on that equipment[28];

---

25 A CNSA survey showed that fifteen out of eighteen responding members prosecuted cases in the period 2003-2006.

26 Directive 95/46/EC.

27 Art. 13 e-Privacy Directive.

28 Art. 5 (3) e-Privacy Directive.

- infecting terminal equipment by inserting **malware** such as worms and viruses and turning PCs into **botnets** or usage for other purposes[29]**;**

- misleading users into giving away sensitive information[30] such as passwords and credit card details by so called **phishing** messages.

Some of these practices also fall under criminal law, including the *Framework Decision on attacks against information systems*[31]. According to the latter, Member States have to provide for a maximum penalty of at least 3 years imprisonment, or 5 years if committed by organised crime.

At a national level, these provisions may be enforced by administrative bodies and/or criminal law authorities. Where this is the case, the **responsibilities of** different authorities and cooperation procedures need to be clearly spelled out. This may require decisions being taken at a high level in national governments.

To date, the increasingly entwined criminal and administrative aspects of spam and other threats have not been reflected in a corresponding growth of cooperation procedures in Member States that brings together the technical and investigative skills of different agencies. Cooperation protocols are needed to cover such areas as exchange of information and intelligence, contact details, assistance, and transfer of cases.

Close cooperation between enforcement authorities, network operators and ISPs at national level is also beneficial for exchange of information, technical expertise and the pursuit of on-line malpractices. Authorities from Norway and the Netherlands have reported on the usefulness of such public-private partnerships.

4.1.3. Resources

Resources are needed to gather evidence, pursue investigations, and mount prosecutions. Authorities need technical and legal resources and must acquaint themselves with the way offenders operate to successfully put their practices to an end.

On-line complaint mechanisms, with associated systems to log and analyse reported malpractices, can be an important tool. Experience has shown that **moderate investments** can bring **significant results**. The reduction in Dutch spam was achieved by establishing a team of 5 full time dedicated employees in OPTA, the Dutch authority, with **€570 000** in equipment to fight spam. Building on this investment, the experience gained in fighting spam is now being used to target other problem areas.

4.1.4. Cross border cooperation

Spam is a global problem. National authorities will often have to rely on authorities in other countries to prosecute spammers, and conversely, may be called upon to pursue investigations coming from other countries.

---

29 *Supra* 28.

30 Art. 6 (a) General Data Protection Directive.

31 Council Framework Decision 2005/222/JHA.

While there may be some reluctance to commit scarce national resources to investigate other people's problems, it is important for Member States to recognise that effective cross-border cooperation is an essential element in fighting spam. Recently the Australian and Dutch spam fighting authorities cooperated in bringing down a large spam operation.

To date 21 European authorities have endorsed the CNSA cooperation procedure[32] on cross border complaint handling; the remaining authorities are invited to do likewise within the next few months. Member States and competent authorities are in particular invited to actively promote the use of:

- the Joint CNSA-LAP pro forma documents

- the OECD Recommendation and Toolkit on spam enforcement.

4.1.5 Proposed actions

Member States and competent authorities are called upon to:

- lay down clear lines of responsibility for national agencies involved in fighting spam

- ensure effective coordination between competent authorities

- involve market players at national level, drawing on their expertise and available information

- ensure that adequate resources are made available to enforcement efforts

- subscribe to international cooperation procedures and act on requests for cross border assistance

4.2. Action by industry

This section covers actions that can be taken by industry to promote consumer trust and mitigate the sending of abusive e-mails.

4.2.1. Software delivery and installation

Spyware poses a serious threat to users' privacy. On-line software offerings have become a much employed method for **delivery and installation of spyware** on user's terminal equipment. Spyware can also be hidden in software distributed through other media such as CD-ROMs for installation on a computer. Unwanted spying programmes may be installed together with the software that the consumer acquires.

To prevent spyware from reaching end-users specific actions are identified below.

4.2.2. Informing the consumer

Software offers may include the installation of additional programmes. Where this added software operates as spyware by monitoring end-users behaviour (e.g. for marketing

[32] *Supra* 18.

purposes) this involves the processing of personal data, and is illegal without the user's informed consent. In many cases, the user's consent to install such software is either not obtained or else is hidden in the small print of a long end-user licence agreement.

Companies that offer software products are encouraged to clearly and prominently describe all the terms and conditions of the offer, in particular if there is processing of personal data by any monitoring devices that are included in software packages.

Self regulation and the use of some sort of 'seal of approval' could provide a means to separate trustworthy companies from those who are not. Codes of conduct, which aim to inform the user on conditions that imply the processing of personal data, can be submitted for endorsement to the Article 29 Data Protection Working Party.

4.2.3 Contract clauses in the chain of supply

Often companies are **not aware** of how advertisements of their products and services are technically being delivered to the public. Legitimate software may be packaged with spyware used to gain access to sensitive data, including credit card data, confidential documents etc.

Companies that advertise and or sell products need to ensure that their contracting parties' activities are legitimate. A company needs to understand the contracting chain of relationships, monitor legal compliance and make malpractice subject to termination throughout the chain, so that further affiliation with mal-practicing companies can be ended immediately.

4.2.4. Security measures by service providers

An ENISA survey in 2006[33] confirms that service providers in general have taken measures to tackle spam. It does however report that service providers could further contribute to the overall security of the network, and recommends that more emphasis is put on filtering e-mail that leaves a service providers network (**egress filtering)**. The Commission encourages service providers to implement this recommendation.

The Article 29 Data Protection Working Party adopted an Opinion on privacy issues related to the provision of email screening services[34] which provides guidance on the question of confidentiality of email communications and, more specifically, on the filtering of on-line communications against viruses, spam, and illegal content.

[33] http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

[34] Opinion 2/2006, WP 118.

4.2.5. Proposed actions

The Commission invites:

- companies to ensure that the standard of information for the purchase of software applications is in accordance with data protection law.

- companies to contractually prohibit illegal use of software in advertisements, monitor how advertisements reach consumers and follow up on malpractice.

- e-mail service providers to apply a filtering policy which ensures compliance with the recommendation and guidance on e-mail filtering.

4.3. Action at European level

The Commission will continue to address the issues surrounding spam, spyware and malware in international fora, in bilateral meetings and where appropriate through agreements with third countries and will continue to foster cooperation between stakeholders including Member States, competent authorities and industry. It will also take new initiatives in the area of legislation and research that aim to provide fresh impetus in the fight against malpractices that undermine the Information Society. The Commission is currently working on the further development of a coherent policy on the fight against cyber crime. This policy will be presented in a Communication planned for adoption in the beginning of 2007.

4.3.1. Review of the regulatory framework

The Commission Communication[35] on the regulatory framework for electronic communications proposes to strengthen the rules in the area of privacy and security. Under the proposal, network operators and service provider would be obliged to:

- notify the competent authority in a Member State of any breach of security that led to the loss of personal data and/or to interruptions in the continuity of service supply.

- notify their customers of any breach of security leading to the loss, modification, access or destruction of personal customer data.

National regulatory authorities would have the power to ensure operators implement adequate security policies and new rules could be established providing for **specific remedies** or an indication of the **level of penalties** to be expected for breaches.

4.3.2. Role of ENISA

The proposals also include a provision recognising the advisory role of ENISA in security matters. Other tasks foreseen for ENISA are outlined in the Commission Communication on a Security Strategy[36] and include:

- to build a trusted partnership with Member States and stakeholders to develop an appropriate **data collection framework** on security incidents and levels of consumer confidence.

---

35 http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm

36 *Supra* 1.

ENISA will closely coordinate that Framework with Eurostat in view of the Community statistics concerning the information society and the i2010 benchmarking framework[37].

- to examine the **feasibility of a European information sharing and alert system** to facilitate effective responses to existing and emerging threats to electronic networks.

4.3.3. Research and development

The forthcoming FP7 program aims at the continued development of knowledge and technologies to secure information services and systems in close coordination with policy initiatives. Topics of work related to malware are expected to include hidden botnets and viruses, and attacks on mobile and voice services.

4.3.4. International cooperation

As the internet is a global network, the commitment to fight spam, spyware and malware needs to be shared around the world. Hence, the Commission intends to reinforce the dialogue and the cooperation with third countries on the fight against these threats and criminal activities that are linked to them. To this end, , the Commission will seek to ensure that spam, spyware and malware is addressed in agreements between the EU and third countries, will seek firm commitment of the most concerned third countries to work with EU member states to fight these threats more effectively, and will closely follow-up the enforcement of jointly committed objectives.

4.3.5. Proposed actions

The Commission will:

- continue efforts in raising awareness and fostering cooperation between stakeholders

- continue to develop agreements with third countries including the issue of the fight against spam, spyware and malware

- aim to introduce new legislative proposals at the beginning of 2007 that strengthen the rules in the area of privacy and security in the communications sector and present a policy on cyber crime

- involve ENISA expertise in security matters

- support research and development in its FP7 program.

5. CONCLUSION

Threats such as spam, spyware and malware undermine the confidence in, and the security of, the Information Society, and have a significant financial impact. While some Member States have taken initiatives, over the EU as a whole **there is insufficient action to address this**

[37] I2010 High Level Group benchmarking framework of 20 April 2006.

development. The Commission is using its role as an intermediary to create greater awareness about the need for greater political commitment to fight these threats.

Enforcement efforts need to be stepped up to stop those who knowingly disobey the law. Further action by industry should be undertaken to complement enforcement activities. Cooperation is needed at national level both within government and between government and industry. The Commission will reinforce the dialogue and the cooperation with third countries and also examine the opportunity to make new legislative proposals and will undertake research actions to further strengthen privacy and security in the electronic communication sector.

Integrated and, where possible, parallel implementation of the actions identified in this Communication can contribute to reducing the threats that are currently compromising the benefits of the Information Society and the economy.
The Commission will monitor the implementation of these actions and assess by 2008 whether additional action is needed.