



EUROPEAN COMMISSION  
Information Society and Media Directorate-General  
Audiovisual, Media, Internet  
**Internet; Network and Information Security**

**REPORT**

**WORKSHOP ON**

**LEARNING FROM LARGE SCALE ATTACKS ON THE INTERNET**

**POLICY IMPLICATIONS**

**17 January 2008**

**DISCLAIMER**

**This report does not necessarily  
represent the views of the Commission**

1.	MAIN OUTCOMES OF THE WORKSHOP .....	2
2.	CONTEXT .....	4
3.	REPORT ON THE SESSIONS.....	5
3.1.	Setting the scene on recent large scale attacks .....	5
3.2.	Lessons learnt in terms of preventive measures .....	7
3.3.	Lessons learnt in terms of detection and response capabilities .....	9
3.4.	Horizontal measures .....	11

## 1. MAIN OUTCOMES OF THE WORKSHOP

On 17.01.08, the European Commission organised a workshop on learning from large scale attacks on the Internet and the policy implications to discuss the lessons learnt and best practices to enhance the security and stability of the Internet. It offered the opportunity to investigate the value of EU and international cooperation as well as Public Private Partnership and it contributed in raising awareness on current Internet security issues.

*Lessons learnt: Critical issues to be considered*

The discussions have shed light on some of the issues the information society is facing regarding Internet's security and reliability.

The **availability and reliability of Domain Name System (DNS)** services have been identified as two key elements for the correct functioning of the Internet. The **security of traffic exchange between operators** of electronic communications networks and in particular the role of the operators of Internet eXchange Points (IXPs) is an other topic which is currently under the scrutiny of some Member States.

Current trends demonstrate that **malware and attacks are becoming very complex and sophisticated**. Attackers exploit to their own benefit the capabilities of Peer-to-Peer (P2P) networks and, increasingly, the opportunities offered by WEB 2.0. Malware development life cycle is gradually more professionalised. The distribution of malware increasingly follows the commercial practices deployed within the software industry (malware toolkits). Some participants noted that attacks do not exploit anything new however. They take advantage of well known vulnerabilities and make use of existing malicious codes. A speaker mentioned that web pages are increasingly becoming the vector for infections.

Another critical issue is the **asymmetric situation** where attackers are always one step in advance compared to the target. Delegates underlined the importance of better understanding attackers and improving capabilities in monitoring networks under attacks.

*Lessons learnt: Current situation*

The **distributed nature of the Internet** was recognised as contributing to its flexibility and resilience. Therefore, if related public policies have to be developed, participants argued that they should respect the distributed nature of the Internet and avoid centralisation.

The discussions also demonstrated that the **distributed nature and openness of the Internet participates in its structural vulnerability**. In that respect, the extent of electronic communications infrastructures was questioned as the computers of end-users (i.e. at the edges) may increasingly be considered as part of the global infrastructure. The distributed nature of P2P is more and more exploited to decentralise the command of malware. As a consequence, attackers are hard if not impossible to identify and deter.

Participants converged in recognising that the **Internet's security and stability is a shared responsibility**. Every stakeholder (public authorities, the private sector and individuals) has a role and responsibility. In that respect, delegates pointed out that the level of security put in place by one entity might eventually brings more benefits to others. This paradox raises the question which incentives should be brought forward to stakeholders to adopt security measures.

## *Lessons learnt: The way forward*

Several participants underlined the crucial necessity to **build further the resilience and robustness of the Internet**. One of the directions proposed was related to ensuring the redundancy of servers and connections. In particular the deployment of Anycast technology was considered valuable to ensure the resilience of DNS services. The value of diversity in the strategies and operations in order to avoid single points of failure, and consequently making it harder for attackers to succeed, was highlighted. The security of routing protocol and traffic exchange would also deserve further attention. Concerning the reliability of DNS services, a delegate mentioned that the deployment of DNS Security Extensions (DNSSEC) has been put into operation in his country.

With regard to malicious activities, the adage "*know your enemies*" was brought to the table by participants who mentioned that behavioural analysis and attackers profiling were key. Delegates pointed out the value and limit of tracking compromised machines. Isolating a country or an organisation to avoid the impact of malicious activities originating from outside the borders was considered unfruitful while amplifying the success of an attack.

At the same time, several participants stressed that **response preparedness is crucial**. The directions mentioned revolve around national contingency plans for the Internet, regular cyber exercises on national/international level and the strengthening of multinational cooperation for rapid response (in a formal rather than informal basis). The importance of building incident response capabilities which could be supported by Computer Emergency Response Teams (CERT), also called Computer Security Incident Response Teams (CSIRT), and their role for national and international cooperation was underlined.

In order to get a better picture of networks' availability and resilience, it is more and more essential to **measure and monitor network traffic**. A "*collective intelligence approach*" was called upon: computers of end users could be leveraged to gather and process the necessary data. Efforts on strengthening early warning systems were considered as crucial to reduce response time and damages. At the same time, the increasing large amount of security information that needs to be analysed is a challenge.

Participants recognised that the **technology will not be sufficient** to reach the adequate level of Internet's security and stability. They highlighted the importance of other aspects:

- Setting-up **Public Private Partnership (PPP)** to build further the resilience of the Internet, prepare the response and improve the understanding of the situation. The role of governments is to coordinate and be a good user;
- Developing cross-sector and cross-organisational **cooperation** at national, European Union (EU) and international levels as well as agreeing on **responsibility's allocation** along the value chain;
- Promoting **information and best practices sharing** for which trust is a precondition; a (legal) framework that permits information sharing was deemed necessary;
- Raising **security awareness and education** of individuals, public bodies, corporate users and service providers;
- Understanding the economics of security and cyber crime.

Eventually, the discussions demonstrated that there is a crucial need to **bridge the gap between policy makers and the technical community**.

## 2. CONTEXT

The European Commission announced in its Commission Legislative Work Programme for 2008<sup>1</sup> the intention to adopt a policy initiative on critical communication and information infrastructures protection (CIIP), under the broader framework of the European Programme on Critical Infrastructure Protection<sup>2</sup>. The objective of this initiative will be to ensure that adequate and consistent levels of **preventive, detection, emergency preparedness and recovery measures** are in place across the EU.

The workshop fostered the discussion on 1) the lessons-learnt from large scales attacks on the Internet and on 2) the best practices devised by stakeholders to enhance the security and stability of the Internet. It offered the opportunity to discuss and investigate the value of EU and International cooperation as well as Public Private Partnership. It also contributed in raising awareness of participants on current Internet security issues.

The workshop gathered 86 participants from Member States bodies, academia, industry and European institutions. The 57 delegates from 21 EU Member States, plus Norway, represented the ministries of defence, interior affairs, industry, communications, finance, or telecom National Regulatory Authorities. Twelve security experts from academia and industry attended the meeting.

The workshop followed the subsequent structure:

- (1) A first session on **setting the scene on recent large scale attacks**. This session is reported in chapter 3.1;
- (2) A track dedicated to **lessons learnt in terms of preventive measures** to mitigate the risks beforehand. This session is reported in chapter 3.2;
- (3) A session on **lessons learnt in terms of detection and response capabilities** to improve preparedness in detecting and responding to incidents. This session is reported in chapter 3.3;
- (4) A track on **horizontal measures**. The session focused on the measures to identify and map stakeholders' roles and responsibilities. This activity is horizontal to the measures aiming to improve prevention, detection and response capabilities This session is reported in chapter 3.4;
- (5) A final session on **the way forward** summarised the outcomes of the workshop. This session is reported in chapter 1 which records the main outcomes of the workshop.

---

<sup>1</sup> See Commission communication - Commission Legislative and Work Programme 2008, COM(2007)640 of 23.10.2007

<sup>2</sup> See COM(2006) 786 of 12.12.2006 and COM(2006) 787 of 12.12.2006

### 3. REPORT ON THE SESSIONS

This chapter presents the views expressed by the participants in the sessions on setting the scene, lessons learnt in terms of preventive measures, detection and response capabilities and the session dealing with horizontal measures.

#### 3.1. Setting the scene on recent large scale attacks

This session provided an overview of large scale attacks on the Internet from three different perspectives: the coordinated cyber attacks against the Internet resources of Estonia, the attacks targeting DNS root servers in 2002 and in early 2007 and the trends in malware propagation.

One of the lessons learnt from the coordinated cyber attacks against the Internet resources of Estonia has been that Network and Information Security is all about trust built on a joint effort. Among other things, the new Estonian cyber security strategy highlights the importance of improving interdepartmental coordination mechanisms for rapid response and recovery. Setting-up incident response capabilities and in particular Computer Emergency Response Teams (CERTs) and developing a cooperation model among them is also crucial to face coordinated attacks. The role ENISA is playing in supporting the coordination between CERTs has been recognised as instrumental.

DNS is another important element of the Internet<sup>3</sup>. Concerning the attacks to the DNS root servers in October 2002 and February 2007<sup>4</sup>, they were actually attacks to the network infrastructure and not to the service itself. It was reported that the DNS services were actually never down. The attacks have demonstrated that it is rather the infrastructure connecting the DNS servers that is vulnerable. It was pointed out nevertheless that the best service is useless if you cannot reach it because the infrastructure is down. Thus, an improvement in the system's infrastructure is needed; in particular, more servers are required to ensure that the services can be reached. The DNS service itself is considered as very resilient by design. Also, with respect to the attack in October 2002, there was no clear picture of the actual damage. To cope with this lack of perception, RIPE developed a better distributed measurement system to assess the availability of DNS service.

Regarding malicious activities on the Internet, one of the speakers pointed out the following trends:

- Attackers are getting more and more professional and sophisticated. The distribution of malware increasingly follows the commercial practices deployed within the software industry via malware toolkits;
- Large botnets have been identified to host 250 000 to 1 million zombie machines. They are mainly used to send spam but also for Distributed Denial of Service attacks;
- Malware functioning is changing from a central command and control architecture to a peer-to-peer architecture;

---

<sup>3</sup> DNS services underpin the resolution of domain names (for instance [www.example.com](http://www.example.com)) into IP addresses which are used by computers to communicate over the Internet.

<sup>4</sup> See ICANN fact sheet at [http://www.icann.org/announcements/factsheet-dns-attack-08mar07\\_v1.1.pdf](http://www.icann.org/announcements/factsheet-dns-attack-08mar07_v1.1.pdf)

- The web is increasingly the vector for infections;
- The number of malware is booming. There is an increasing trend in the number of bots and Trojan horses and a decreasing one in the number of viruses and worms. The anti-malware industry was reported as facing difficulties to keep up with the overload of malwares;
- The effectiveness of anti virus is unfortunately reducing and a new strategy should be considered. A speaker mentioned that a study has evaluated that approximately 40% of analysed computers have updated anti-viruses installed and, up to 15 to 20% of the computers with updated anti-viruses protection might be infected with active malware;
- We should not forget that there is also an increasingly large number of small scale attacks occurring (not just large scale ones).

The speakers and the participants proposed some directions to be followed. Better technology approaches based on collaborative intelligence and behavioural analysis should be considered. With a collective intelligence approach it would be possible to correlate data, through different sensors installed on the network, responsible for collecting data and sending it to a machine to process it. Computers at the edges could be leveraged to build this collective intelligence.

Behavioural analysis and profiling attackers is essential to understand attackers' motivations and consequently better protect the infrastructure. It was reported that a Europol working group is working on profiling cyber attackers.

At the same time, it would be needed to foster cooperation between jurisdictions. In particular, Internet Service Providers (ISP) should be able to share information in order to be able to respond effectively. The help of domain registrars would also be valuable to report on rapid changes of domain information. Moreover, the importance of the existence of multinational rapid response teams cooperating on a formal rather than informal basis was highlighted.

Encouraging the hardening of networks was also considered as a necessary step to enhance Internet's resilience. Proposed technical solutions included the deployment of Anycast and ensuring redundancy of servers and connections. Participants pointed out, however, that the motivation for hardening the networks could be impaired by the fact that, sometime, the hardening brings more value to others than to the one putting it in place; the benefits might not be local but remote. Therefore, it is important to involve all stakeholders in making an effort to contribute to the same objective, possibly through public-private partnerships.

In addition, participants have put forward several policy options to be considered in mitigating attacks. Firstly, take advantage of the technology and implement measures at ISP level to decrease malicious traffic. Secondly, implement better domain registration controls to impede malicious activities. Finally, extend regular vulnerability scans to all businesses with web sites.

It was also mentioned that the Internet is not a self-organising and self-fixing network as theoretically portrayed. The distributed nature of the Internet should be hailed for the role it plays in contributing to more flexibility and resilience. Therefore, if related public policies have to be developed, participants commented that they should respect the distributed nature of the Internet. Plans for centralisation should be avoided.

### **3.2. Lessons learnt in terms of preventive measures**

The session first dealt with measures to enhance the robustness of the infrastructure underlying the Internet (DNS security, redundancy of links, etc). The second part covered measures to enhance the security of servers which host the web sites composing the Internet.

#### **Development and deployment of measures to protect Internet infrastructure**

The Swedish experience in building a strategy to improve Internet security was presented. As preventive measures, Sweden focused on building rock shelters for ISP equipment as well as extra redundancy in network infrastructure (with the financial support of the government) and ensuring cooperation between telecom and electricity suppliers. The later 2006 government's strategy for a more robust and resilient Internet infrastructure has put forward preventive measures that include the following: a recommendation for providers of services to increase website accessibility, a new law to ensure better management of the national Top-Level Domain, the promotion of Domain Name System Security Extensions (DNSSEC) deployment and use, the improvement of security at the traffic exchange points between ISPs, the creation of a contingency plan for the Internet and the establishment of a National Crisis Management Group. The success of public-private partnerships in the development and implementation of better crisis management and in facilitating actions for security and robustness was pointed out.

While the current level of availability of the DNS service was considered as becoming less problematic, the lack of reliability of the DNS responses was pointed out in contrast. It was questioned whether DNSSEC could help improving the situation by ensuring that the responses from the DNS server can be trustworthy through digital signatures. Concerning availability, more geographical distribution should be promoted. Anycast is a proven technical solution that might help building redundancy. Having an Anycast server closer to the source of attack (from a network topology perspective) will attract the "bad" traffic of an attack and therefore its global impact will be reduced. In the same way, being able to resolve all the world's domain names at a local level reduces the opportunity for attacks on DNS global infrastructure. Service providers should also use and deploy multiple platforms (software and hardware), from different sources, to reduce exposure. A key principle is to avoid single points of failure.

The Border Gateway Protocol (BGP) was also considered insecure entailing the risk of generating false routes at Internet eXchange Points (IXP). Attention was drawn to safeguard the routing between ISPs. To this end, Internet eXchange Points operators should build efforts to offer greater peering capabilities through stable and resilient peering platforms.

Views on how to protect Internet infrastructure have identified the importance of staying ahead of crime through ongoing infrastructure investment, continuous monitoring and analysis of traffic trends. Multiple platforms should be deployed in multiple locations. Early warning should be based on information sharing to identify likely types of attacks. It was also remarked the value of diversity in the strategies and operations in order to avoid single points of failure, and making it harder for attackers to succeed. In this context, isolating a national network that is under attack does not help mitigating the problem, but rather increases the chances of attackers to achieve their objectives. Moreover, there was also the view that as long as cyber-crime is a driver, then the infrastructure is normally safe, because its integrity and availability is also needed to perpetrate attacks.

Conducting and learning from international exercises were also considered as vital to ensure preparedness and better response in the event of attacks.

### **Measures to protect the provision of web services**

The approach of CERTA, the French CSIRT, in improving Internet security was presented. CERTA prevents and deals with security incidents, and informs and trains citizens about trends and vulnerabilities. It also promotes real-case scenario exercises involving ministries and contributes to end-users education.

Participants highlighted the role of security intelligence in becoming pro-active towards security. An example of a large global intelligence network was presented. The network is composed, among other elements, by 40 000 registered sensors in more than 180 countries, 8 security responses centres distributed around the globe and it monitors 30 % of world's e-mail traffic.

Security firms report that attacks are getting more and more sophisticated. In the last six months most of the attacks used malware toolkits like MPack. In fact, most of the massive attacks are not using anything new, but well known vulnerabilities and malicious codes. The vulnerabilities of Web 2.0 are also more and more exploited. It was remarked that underlying web applications are not always receiving the same level of security auditing as traditional client-based applications.

Conclusions about measures to protect web services suggested the following:

- Both large and small providers should uniformly adopt security measures;
- Service providers should follow standards. The adoption and compliance to ISO/IEC 27001 and ISO/IEC 27002 should be promoted;
- Software best practices and robust services are needed;
- The role of security intelligence is crucial to become pro-active;
- National and International cooperation is key. In that respect the importance of CERTs and National Centers for the Protection of the Critical Infrastructure was underlined;
- Re-enforcing cooperation within a clear legal framework between law enforcement authorities, governmental CERTs and the private sector is needed;

Once again, the distributed nature of the Internet and the high dependency chain involved, as well as, the shared and distributed responsibility towards the Internet were pointed out. In the case of public-private partnerships, governments should not only play a role of coordinators but also of good users. Trust between stakeholders is crucial especially when it comes to cooperation.

The importance of learning from the experience of the financial sector, which is suffering hundreds if not thousands of targeted attacks a day, was also pointed out.

Eventually, it was questioned again which incentives should be brought forward to stakeholders to adopt security measures considering that the level of security put in place by one entity is not strictly local but would eventually bring benefits to the others.

### **3.3. Lessons learnt in terms of detection and response capabilities**

The session first dealt with large scale detection systems and early warning systems that can be used to support national and European strategies. The second part dealt with procedures and mechanisms to structure response activities and damage limitation across Member States.

#### **Detection and early warning and alert systems**

Having an early warning system in place to be able to respond faster and to control the damage is crucial. The main objectives of such early warning system should be, *inter alia*, to improve the scope of detection capabilities through the installation of more probes in the network, improve response time in order to reduce the impact of attacks, and strengthen international cooperation.

The Dutch experience suggested that combining efforts with other CERTs to set up a Pan-European early warning system ("*Pan-European dashboard*") could be of great interest.

It was also reinforced the need for more and better collaboration between stakeholders and the need to extend it to an international level, as it is assumed that large scale attacks will tend to always have an international component. Collaboration today is mainly based on the efforts of ENISA, EGC (European Government CERTs), TFCSIRT (Terena's taskforce to promote collaboration between European CERTs), FIRST (international forum of CERTs) and on ad-hoc relationships.

Thus, a trusted and reliable international network, based on formalised collaboration and information sharing, was called for. The overall strength could be built on each CERT unique qualities. A complete and reliable network of contacts in Member States would facilitate the task. It was noted however that not all countries foresee to have central contacts. It was also requested more support and funding for CERTs to fight cyber crime while nowadays this type of funding is mainly directed to intelligence and police. A definition of which CERT capabilities could be attributed to European Community agencies should be decided. For what concerns information sharing, the attention was drawn on the creation of technical and legal mechanisms to encourage and help organisations to share and exchange attack-related data and to put in place a legal framework for data sharing that clearly defines who, when and for which purpose can data be accessed.

#### **Readiness to react to attacks relayed by large number of distributed sources**

In this session, the lessons learnt from the large scale attacks against Hungarian banks and Estonia's Internet resources were presented.

A few years ago seven Hungarian banks were the target of a large scale phishing attack executed by international botnets during two weeks. Stakeholders involved in mitigating the problem included the banks, national and international CERTs, ISPs and law enforcement agencies. The lessons retained from these attacks are the importance and need for enhanced level of preparedness, early warning, manpower, coordination, involvement with international partners and media work.

The Estonian attack was conducted by circa 4000 compromised machines and affected the country's infrastructure. Compared to other large scale attacks, the Estonian incident was relatively small, but it was just right for the scalability of the national infrastructure,

resulting in a considerable impact. Stakeholders involved in the incident response consisted of CERTs (the Estonian one as well as experts from the international CERT community) and ISPs. Lessons learnt from this attack revealed the importance of fast incident response capability and of CERT organisations and, most of all, the cooperation/communication between them. The global extent of the Internet also calls for international cooperation and international contingency plans.

Recommendations to tackle large scale attacks from distributed sources put forward by participants comprised the following:

- Foster dialogue for policy making, e.g. by a EU Platform for ISPs, owners of Critical Infrastructures, governments and CERTs;
- Recommend a model for EU operational coordination based on best practices, in the financial sector and in particular via Information Sharing and Analysis Centres Councils;
- Promote European exercises involving large industry players, Member States and EU agencies on a voluntary basis;
- Support voluntary cooperation between Member States' early warning systems;
- Redefinition of critical infrastructure to include private and business infrastructures, considering the impact of personal computers in this type of attacks;
- Have contingency plans to maintain the Internet within the country and survive without the outside Internet;
- Facilitate law enforcement cooperation globally.

### **3.4. Horizontal measures**

This session covered the identification and mapping of stakeholders' roles and responsibilities. This topic is horizontal to measures aiming to enhance the prevention, detection and response capabilities.

The German Implementation Plan for Critical Infrastructure Protection (CIP) was introduced. The main ideas that have been put forward in the plan revolve around recognising that the security of critical infrastructures is a joint responsibility, trust is crucial and cross-sector and public-private collaboration is necessary. This implementation plan has been drafted in cooperation between a large number of critical infrastructure operators and public administrations. It is based on the need to address protection of information infrastructures, preparedness in response to IT (Information Technology) incidents and sustainability, in particular, in ensuring IT competence. The role of the government in defining the CIP strategy and in operating a situation room and analysis centre, as well as, the role of the operators/owners of critical infrastructures in implementing the strategy and the recommendations proposed in the CIP Implementation Plan were underlined.

ccTLD (country-code Top Level Domains) registries should invest in systems resilience to ensure the security and resilience of the Internet. Systems resilience is built via correct dimensioning, connectivity and redundancy, rather than in improving the DNS system itself, as the latter is supposed to be resilient in its design by providing caching and redundancy.

For what concerns the role of ISPs, it was pointed out that the word ISP encompasses a wide range of actors, i.e., access providers, hosting providers, email service providers, online service providers, etc. ISPs aim for self-regulation. For instance, business continuity plans should be internally developed in order to deliver the capability of reacting rapidly to unexpected and unpredictable attacks. It is also desirable to have comprehensible legislation and regulation in place. In that respect, bridging the gap between policy makers and the technical community is crucial.

As a conclusion all participants reiterated that IT security is a shared responsibility and can only be guaranteed if all stakeholders accept their responsibilities and build up mutual trust and understanding. Another important component is national cooperation between all the stakeholders. Cooperation needs to be extended to an international level too, as the global character of the Internet does not permit one country isolating itself from the Internet.