enisa
European Network
and Information
Security Agency

Protecting Europe's Citizens against Cyber Attacks

2008

ENISA and Network & Information Security

Every day, we take for granted innovations offered by mobile technology, e-communications and the Internet. Individuals and companies alike are growing increasingly 'digitally dependent' as 30% of global trade relies on the internet. Network and information security (NIS) is therefore critical both to protect privacy and build trust in e-channels, as well as to ensure the effective functioning of Europe's internal market.

As networks become more complex, they grow in vulnerability. Security breaches and cyber attacks result in substantial economic damage on an individual, organizational and national level. **In short, NIS is a concern for everyone.**

ENISA is a European Union (EU) expert body in NIS. In addition to promoting best practice, the Agency provides independent advice to the EU on NIS, responds to Member States requests, and collects and analyses data on incidents and emerging risks.

Data Collection of Security Incidents

Security incidents are difficult to quantify. Service providers are sometimes reluctant to report episodes due to the potential brand impact, while governments are not motivated to release information on security breaches. ENISA conducted a feasibility study on an EU-wide partnership for the establishment of a data collection framework on security incidents. While a single partnership is not feasible, the EU can create new, or build on existing, partnerships. In a common *platform*, public and private partners can share and analyse past breaches and possibly anticipate future trends and emerging risks, improving the resilience of, and confidence in, ICT in Europe.

Network Vulnerabilities

Networks and service providers face a host of challenges, including viruses, spam, distributed denial of service attacks (DDoS) and worms. Whiles viruses represent the most pervasive threat, spam continues to be a concern. For example, as less spam reaches its target – only 6% of all e-mail traffic actually reaches mailboxes – the public perceives the situation to be under control. The reality is, however, that spam is growing in quantity, size and bandwidth and remains a costly problem. Ferris Research estimated that spam would cost businesses around €64,5BN in 2007, double the 2005 figure.

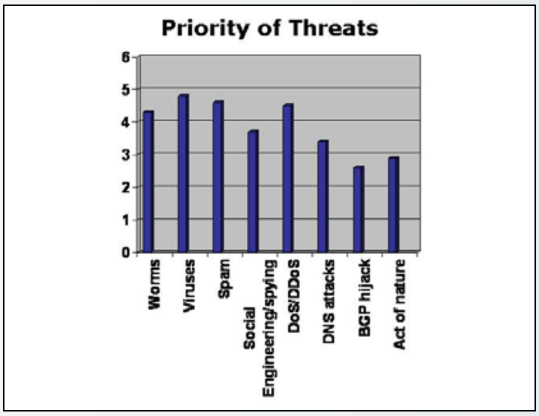

Figure 1: Priority of security threats faced by service providers

Botnets are another insidious threat. Remotely managed from a 'command and control' server by criminals, botnets are 'hijacked' computers used for fraudulent online activity. Bots are silently installed (60% via browser exploitation) and remain unnoticed by the owner of the infected computer. A compromised computer can be involved in any kind of online criminal activity: identity theft, unsolicited commercial e-mails, scams, and massive attacks. Regardless of the motive, cyber attacks can be a serious disruption to business and impact on people's daily lives. ENISA estimates that 6 million computers have been hijacked worldwide.

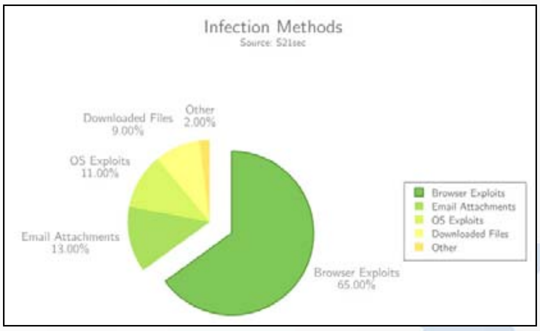

Figure 2: Most common bot infection methods as detected by S21sec

Countering NIS threats

Massive cyber attacks can never be totally prevented but ENISA is working on a three year programme to support the Member States by collectively evaluating and improving the resilience of Europe's public e-communication networks and services through promotion of best practice. The aim is that by 2010, 50% of all Member States will implement ENISA's recommendations in policy-making.

ENISA calls for mandatory reporting of security measures and breaches

The Agency is examining security risks and solutions beyond 2008 in the areas of:

- mobile identity management looking at portable devices/applications involving collection and control of personal data;
- Web 2.0, such as rich, browser-based applications;
- operating system (i.e., x86 platforms) virtualisation technologies; and
- virtual worlds and online gaming, with an estimated value in 2006 of between €64,5M and €100M per year.

As small- and medium-sized enterprises (SMEs) represent 99% of all business in the EU and 2/3 of private sector jobs, ENISA is working to raise awareness of security issues amongst this audience. ENISA recognizes that SMEs need ready-to-use, easy solutions and is examining the prospects of an EU-wide network also for micro-enterprises. ENISA has conducted a feasibility study into the establishment of a European Information Sharing and Alert System (EISAS) on threats, vulnerabilities and attacks. As they are easy victims, home users and SMEs are the most popular targets of cyber attacks. ENISA found that the EU should assume the role of facilitator, moderator of discussion and guardian of good practice between national information sharing and alert systems.

I want to know more…

- Position paper on reporting of security measures and breaches: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_strengthening_eu_legislation.pdf
- Position paper on Botnets: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf
- Study examining the feasibility of a Data Collection Framework: http://www.enisa.europa.eu/doc/pdf/studies/data_collection_report_20080214.pdf
- Improving resilience of Europe's e-communications http://www.enisa.europa.eu/pages/resilience.htm
- Study on security and anti-spam measures: http://www.enisa.europa.eu/pages/spam/doc/enisa_spam_study_2007.pdf
- Feasibility study on EISAS: http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf

Please visit our website regularly (http://www.enisa.europa.eu), or email us at info@enisa.europa.eu).