Executive Summary

Spurred by the prevalence of always-on, high-speed connections, the Internet has become a powerful tool for enhancing innovation and productivity. The increasing dependence on the Internet and other communication networks, however, means the Internet has also become a popular and efficient way to distribute computer viruses and other types of malicious software.

"Viruses", "worms" and "zombies" might sound like science fiction, but they are in fact the reality presented by the spread of malware. The power and threat of malware are that it can infiltrate, manipulate or damage individual computers, as well as entire electronic information networks, without the users' knowing anything is amiss.

All of this has brought the electronic world to an important juncture. The onslaught of malware attacks is increasing, both in frequency and sophistication, thus posing a serious threat to the Internet economy and to national security. At the same time, current efforts to fight malware are not up to the task of addressing this growing global threat; malware response and mitigation efforts are essentially fragmented, local and mainly reactive.

This report is a first step toward addressing the threat of malware in a comprehensive, global manner. As such, the report has three major aims: (1) to inform policy makers about malware – its growth, evolution and countermeasures to combat it; (2) to present new research into the economic incentives driving cyber-security decisions; and (3) to make specific suggestions on how the international community can better work together to address the problem.

The need for a consistent approach to a global problem is not new, but malware presents particular challenges owing to the wide variety of actors working on the problem: governments, businesses, end users and the technical community. These different actors need to improve their understanding of the challenges each of them faces and to co-operate, within their communities and across communities. Furthermore, this co-operation must occur at the global level. It is not enough for one country or one community to effectively self-organise if others do not do so as well.

In light of the need for a holistic and comprehensive approach to malware, a common point of departure is needed from which to build co-operation and collective action. This report calls for the creation of a global "Anti-Malware Partnership" involving governments, the private sector, the technical community and civil society.

The rise of malware

No longer limited to the realm of computer hackers and tech researchers, malware in the 2000s has become a serious business and a multi-million-dollar criminal industry. The major drivers can be summarised as follows:

Malware is widely available. Virtually anyone can buy it online at a nominal cost, as well as from underground markets. And malware is user-friendly, meaning it provides attackers with the capability to launch prolonged, sophisticated attacks beyond their skill level.

Malware can infect all sorts of devices. Since it is nothing more than a piece of software, malware can infect not only personal computers but also the backbone of the Internet – the servers and routers that move data worldwide. While malware often propagates through the Internet, it is important to note it can also be introduced into computer systems not connected to the Internet.

Malware is profitable. Together with other cyber tools and techniques, malware is a low-cost, reusable way to carry out highly lucrative forms of cybercrime. Two prime examples are the capture of credit card and bank account data via "spyware" and the launch of "denial-of-service" attacks used to extort money or concessions.

The costs

Malware can harm critical information infrastructures, cause major financial losses and, perhaps worst of all, undermine trust and confidence in the Internet economy. Therefore, malware is increasingly a shared concern for all Internet market participants: governments, businesses and individuals in both OECD countries and Asia Pacific Economic Co-operation (APEC) economies.

Governments, for one, are increasingly dependent on the Internet for providing services, making them and their citizens vulnerable to malware. In addition to the complex and expensive task of securing their own systems, governments are being called upon to protect the general public from online ID theft and other Internet crimes.

Malware is also taking a toll on the private sector. With few exceptions, many private Internet market participants – from Internet Service Providers

to e-commerce companies to software vendors – have had to increase security-related investments in order to expand their online business.

The key Internet market participants interviewed for this book (please see Part II) were devoting an estimated 6% to 10% of their technology budgets to protect against malware. Combined with indirect costs (such as funding watchdog organisations, public education campaigns and law enforcement efforts) the total costs of malware for key Internet market participants may well be above 10% of technology spending.

Problematic trends

As explained in Part I, the deployment of malware is becoming ever-more sophisticated and targeted, presenting a great challenge to those attempting to measure and combat the problem. Key findings include:

- Self-sustaining cyber attacks increasingly depend on "botnets", or groups of malware-infected computers (also called "zombies") that can be used to remotely carry out attacks against other computer systems.
- Many malware attacks are smaller and deliberately limited in scope, in an attempt to stay "below the radar" of the security and law enforcement communities.
- Spam has evolved from a nuisance, to a vehicle for fraud, to a vector for distributing malware.
- The overall malware problem is difficult to quantify: no single entity has a global understanding of the scope, trends, development and consequences of malware.
- Data on malware are not consistent, and terminology for cataloguing and measuring the occurrence of malware is not harmonised.
- The effectiveness of current approaches in combating malware is constantly challenged by both ongoing technological changes and faster exploitation of software vulnerabilities.

The role of economic incentives

To a great extent, cyber security is affected by the behaviour of the key Internet market participants: Internet Service Providers; e-commerce companies; domain name registrars; software vendors; and end users. Part II of this book presents new field research on how these Internet market participants make their information-security decisions.

During 2007, 41 in-depth interviews were conducted with organisations confronted with malware. In each instance, the following questions were asked: how the organisation is confronted with malware; what its responses

are; what trade-offs are associated with these responses; and how the organisation is affected by the security actions of other market participants. Some key findings were:

- How key market participants address malware is greatly influenced by the specific incentives they face: greater online traffic vs. higher security costs, for example. Some of these incentives work to enhance online security while others work to reduce it.
- In many instances, market participants make decisions that pass on the costs of malware to others in the network (thus "externalizing" them), such as when end users opt not to protect their computers against viruses.
- Owing to existing feedback loops, which should be strengthened and expanded, the extent of passed-on costs and benefits is probably smaller than had been previously assumed. On the other hand, many of these passed-on costs remain unaddressed.

A global approach

While this work details many of the problems presented by malware, it is only a first step towards a solution. To prevent malware from becoming a serious threat to the Internet economy and to national security, a global partnership against malware is needed.

A wide range of communities and actors – from policy makers to Internet Service Providers to end users – all play a role in combating malware. But there is still limited knowledge, understanding, organisation and delineation of the roles and responsibilities of each of these actors.

Therefore, a global "Anti-Malware Partnership" should involve not only governments, but also the private sector, the technical community and civil society. Such an inclusive, co-ordinated effort would be more likely to produce co-ordinated policy guidance to fight malware on all fronts – from educational to technical to legal and economic.

This type of international co-operation should be supported and enhanced by accurate measurement of the problem and analysis of the underlying economics at play. Also, the limitations of current actions against malware should be addressed, and the question of how to strengthen anti-malware incentives for market participants should be further explored.

Improvements can be made in many areas, and international co-operation would benefit greatly in areas such as: proactive prevention (education, guidelines and standards, research and development); improved legal frameworks; stronger law enforcement; improved tech industry practices; and better alignment of economic incentives with societal benefits.

Background

The Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP) and the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG) have both experience and expertise in the development of policy guidance for the security of information systems and networks.

In 2002, the OECD adopted the *Guidelines for the Security of Information Systems and Networks* ("the *Security Guidelines*") which provide a clear framework of principles at the policy and operational levels to foster consistent domestic approaches to addressing information security risks in a globally interconnected society. More broadly, the *Security Guidelines* reflect a shared ambition to develop a culture of security across society, so that security becomes an integral part of the daily routine of individuals, businesses and governments in their use of Information and Communication Technologies (ICTs) and in conducting online activities.[1] In 2003 and 2005, the OECD monitored efforts by governments to implement national policy frameworks consistent with the *Security Guidelines*, including measures to combat cybercrime, develop Computer Security Incident Response Teams (CSIRTs), raise awareness, and foster education as well as other topics (OECD, 2005a). In 2006 and 2007, the OECD focused on the development of policies to protect critical information infrastructures (OECD, 2007c and 2008).

Likewise, in 2002, APEC issued the APEC Cybersecurity Strategy outlining six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education. To supplement the APEC Cybersecurity Strategy, in 2005 the APEC TEL adopted the Strategy to Ensure a Trusted, Secure, and Sustainable Online Environment to encourage APEC economies to take action for the security of information systems and networks.

Shared OECD and APEC objectives

In 2005, the APEC and OECD co-organised a workshop to share information on evolving information security risks and to explore areas for further co-operation between the organisations to better tackle the international dimension of information security risks. In 2006, both organisations agreed that the need to encourage a safer and more secure online environment was more pressing than ever due to the continued growth of economic and social activities conducted over the Internet and the increased severity and sophistication of online malicious activity. Subsequently, they decided to organise a workshop[2] and develop an analytical report to examine the issues of malicious software, commonly known as "malware", with a view to:

- Informing national policy makers on the impacts of malware.
- Cataloguing trends in malware growth and evolution.
- Examining the economics of malware and the business models behind malicious activity involving malware.
- Evaluating existing technical and non-technical countermeasures to combat malware and identify gaps; and,
- Outlining key areas for action and future work.

Prepared by the OECD Secretariat in close collaboration with volunteer government experts from OECD and APEC as well as the private sector, this report does not discuss every aspect of malware, all types of malware, or all propagation vectors. Rather, it focuses on issues of significant concern and areas which may pose problems in the future. Similarly, the report does not examine all possible strategies associated with preventing, detecting and responding to malware but rather focuses on elements of relevance to OECD member countries, APEC economies, and other governments and organisations more broadly. Finally, the report refers to forms of cybercrime, such as spam and phishing[3] that may not *directly* involve the use of malware but nevertheless demonstrate how malware can also be used *indirectly* to facilitate cybercrime.

Notes

1. The United Nations, the Council of the European Union, the Asia Pacific Economic Co-operation (APEC) and the Asia-Europe Meeting (ASEM) all recognised and used the Guidelines in their work.

2. Information on the joint APEC-OECD Malware Workshop is available at: *www.oecd.org/document/34/0,3343,en_2649_34255_38293474_1_1_1_1,00.html*.

3. Phishing refers to a social engineering attack, where an attacker manipulates a user to disclose their online account access credentials or other personal information (typically) to a website in the control of an attacker. According to this definition phishing may not *directly* involve malware. However, when the term is used to, for example, also refer to certain types of Trojan attacks, malware is implicated.

Glossary of Malware Terms

Authentication factors: Used to obtain access; something the user knows (such as a password); something the user has (such as a credit card or token); or something the user is (a photograph or thumbprint).

Authentication/Authenticity: Being able to prove or verify a person's or entity's identity with a certain level of assurance. Authentication mechanisms are used to provide access control to information systems.

Availability: Ensuring that digital data within an information system and the system itself are available to authorised users.

Backdoors[1]: A backdoor is malicious code that allows unauthorised access to a computer system or network by accepting remote commands from an attacker elsewhere on the Internet.

Bluejacking: Sending unsolicited messages to Bluetooth connected devices.

Bluesnarfing enables unauthorised access to information from a wireless device through a Bluetooth connection.

Bot programme: A type of 'backdoor' programme that allows attackers to remotely control many compromised information systems (often thousands) simultaneously (or individually).

Botnet(s): Group of malware infected computers that can be used to remotely carry out attacks against other computer systems.

Confidentiality: Being able to protect information and data from unauthorised access.

CERTs: Computer emergency response teams.

CSIRTs: Computer security incident response teams.

DDoS: Distributed denial of service attacks.

1. NIST (2005), pp. 2-12.

Digital certificate: A means of authenticating an identity for an entity when doing business or other transactions on the web or on line. Digital certificates exist as part of public key infrastructures (PKI).

Domain name: The identifier or address of any entity on the Internet. Domain Name System (DNS): The way Internet domain names are located and translated into an Internet Protocol, or IP, address. For example, the domain name www.oecd.org is a more user friendly and memorable alternative to the IP address 193.51.65.71.

Honeynet: Two or more honeypots on a network form a honeynet.

Honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated, (un)protected and monitored, and which seems to contain information or a resource that would be of value to attackers.

Integrity: A primary security goal of information systems which seeks to ensure that the system as a whole (people, data, software) have not been compromised and can continue to be trusted. Internet Protocol The native language of programmatic communication on the Internet.

Keystroke loggers[2] *:* A hidden programme that records and "logs" each key that's pressed on the compromised system's keyboard, as the legitimate user of the system is typing.

Malware payload: The primary function of a piece of malware.

Non-repudiation: A security goal which seeks to prevent a person from denying they undertook an electronic transaction when they did.

Operating system: A computer program that manages the hardware and software on a computer.

Packet: The minimum autonomously-routable quantum of data which can be transmitted across a modern digital "packet switched" network.

Patch/Workaround: A small piece of software code designed to correct or rectify an existing bug or flaw in an operating system or application programme. A work-around is a set of actions that network security managers can take to reduce their exposure to a known software vulnerability.

---

2. Ibid.

Payload: The essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination.

Rootkit: A set of programmes designed to conceal the compromise of a computer at the most privileged "root" level, by modifying operating system files or inserting code into the memory of running processes.

Social engineering: Techniques designed to fool human beings into providing information or taking an action that leads to a subsequent breach in information systems security.

Spam: Commonly understood to mean bulk, unsolicited, unwanted and potentially harmful electronic messages.[3]

Spoofing is a technique designed to deceive an uninformed person about the origin of, typically, an e-mail or a website.

Spyware: A form of malware that is capable of capturing a range of data from user input (keyboards, mice) and output (screens) and other storage (memory, hard drive etc.) and sending this information to the attacker without the user's permission or knowledge.

Transaction signing: The process of calculating a keyed hash function to generate a unique string that can be used to verify both the authenticity and integrity of an online transaction.

Trojan horses: A computer program that appears legitimate but actually has hidden functionality used to circumvent security measures and carry out attacks.

Virus: Directly analogous to its biological namesake, a virus is hidden code that spreads by infecting another program and inserting a copy of itself into that program.

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management of software that could be exploited.

Worm: A type of malware that self replicates without the need for a host programme or human interaction.

3. OECD (2006).

Bibliography

A-i3 (2006), Zur Haftung von Phishing-Opfern. *Arbeitsgruppe Identitätsschutz im Internet e.V, www.a-i3.org/content/view/975/230/.*

Anderson, R. (2001), "Why Information Security is Hard: An Economic Perspective", Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, IEEE Computer Society, *www.acsac.org/2001/papers/110.pdf.*

Anderson, R. (2002), "Unsettling Parallels between Security and the Environment", First Annual Workshop on Economics and Information Security, *www.cl.cam.ac.uk/~rja14/econws/37.txt*.

Anderson, R. (2007), "Closing the Phishing Hole – Fraud, Risk and Nonbanks", *www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf*.

Anderson, R. and T. Moore (2006), "The Economics of Information Security", *Science*, 314: 610-613.

Anderson, R. and T. Moore (2007), "Information Security Economics – and Beyond", Computer Laboratory, University of Cambridge, *www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf*.

Anderson, R., *et al.* (2008), "Security Economics and the Internal Market", European Network and Information Security Agency, *www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf*.

APACS (2008), "Fraud abroad pushes up losses on UK cards following two-year fall", press release, *www.apacs.org.uk/2007Fraudfiguresrelease.html*.

APWG (Anti-Phishing Working Group) (2006a), *Phishing Activity Trends Report*, *www.antiphishing.org/reports/apwg_report_april_2007.pdf*, last accessed 14 December 2007.

APWG (2006b), *Phishing Activity Trends Report, www.websense.com/securitylabs/resource/PDF/apwg_report_december_2006.pdf*, last accessed 14 December 2007.

Arbor Networks (2007), *Worldwide Infrastructure Security Report, Volume III*, *www.arbornetworks.com/report*.

August, T. and T. I. Tunca (2006), "Network Software Security and User Incentives, *Management Science*, 52(11): 1703–1720.

AusCERT (2005), "Windows Rootkit, Prevention, Detection and Response", *www.auscert.org.au/*, last accessed 11 December 2007.

AusCERT (2006), "Haxdoor – An anatomy of an online ID theft Trojan", *www.auscert.org.au/render.html?cid=1920*, last accessed 10 December, 2007.

Australian Government, Office of the Privacy Commissioner (2004), *Community Attitudes towards Privacy 2004, www.privacy.gov.au/publications/rcommunity/chap10.html*, last accessed 11 December 2007.

Bangeman, E. (2006), "Court likely to order ICANN to suspend Spamhaus' domain", *Ars Technica*, *http://arstechnica.com/news.ars/post/20061009-7938.html*.

Banktip (2006). "Phishing: Kunden haften für Trojaner", Banktip.de, *www.banktip.de/News/20648/Phishing-Kunden-haften-fuer-Trojaner.html*.

Barnum, S. and M. Gegick (2005), *Economy of Mechanism*, Build Security In, *https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/348.html?branch=1&language=1*.

Bauer, J. M., *et al.* (2008), "Financial Aspects of Network Security: Malware and Spam", International Telecommunication Union, July, *www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf*.

BBC News (2004), "MyDoom virus biggest in months", BBC News website, *http://news.bbc.co.uk/1/hi/technology/3432639.stm*, last accessed 14 December 2007.

BBC News (2007a), "Google searches web's dark side", BBC News website, *http://news.bbc.co.uk/2/hi/technology/6645895.stm*.

BBC News (2007b), "Burgers paid for by mobile phone", BBC News website, *http://news.bbc.co.uk/2/hi/technology/6400217.stm*, last accessed 7 December, 2007.

Becker, G. S. (1968), "Crime and Punishment: An Economic Approach", *The Journal of Political Economy*, 76(2): 169-217.

Becsi, Z. (1999), "Economics and Crime in the States," *Economic Review - Federal Reserve Bank of Atlanta*, 84(1): 38-56, *http://ezproxy.msu.edu:2047/login?url=http://proquest.umi.com/pqdweb?did=40779835&Fmt=7&clientId=3552&RQT=309&VName=PQD*.

Berner, R. and A. Carter (2005), "The truth about credit-card fraud", *Business Week Online*, *www.businessweek.com/technology/content/jun2005/tc20050621_3238_tc024.htm*.

Bernstein, D. J. (2007), "Some thoughts on security after ten years of qmail 1.0", 1st Computer Security Architecture Workshop in conjunction with 14th ACM Conference on Computers and Communication Security, Fairfax, Virginia, *http://cr.yp.to/qmail/qmailsec-20071101.pdf*.

Böhme, R. (2005), "Cyber-Insurance Revisited", Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/15.pdf*.

Brendler, B. (2007), "Spyware/Malware Impact on Consumers"; APEC-OECD Malware Workshop, StopBadware Project, April, *www.oecd.org/dataoecd/33/55/38652920.pdf*, last accessed 13 December 2007.

Camp, L. J. (2006), *Mental Models of Privacy and Security*, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=922735*.

Camp, L. J. and C. Wolfram (2004), *Pricing Security: Vulnerability as Externalities*, *http://ssrn.com/abstract=894966*.

Campbell, K., *et al*. (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", *Journal of Computer Security* 11(3): 431-448, *http://brief.weburb.dk/archive/00000130/01/2003-costs-security-on-stockvalue-9972866.pdf*.

Cavusoglu, H., B. Mishra and S. Raghunathan (2004), "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *International Journal of Electronic Commerce*, 9(1): 69, *www.gvsu.edu/business/ijec/v9n1/p069.html*.

Cavusoglu, H., H. Cavusoglu and S. Raghunathan (2005), *Emerging issues in responsible vulnerability disclosure*, Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/cavusoglu.pdf*.

CERT (United States Computer Emergency Response Team), Federal Incident Reporting Guidelines, *www.us-cert.gov/federal/reportingRequirements.html*.

CERT Coordination Center (2006), List of CSIRTs with national responsibility, www.cert.org/csirts/national/contact.html, last accessed 10 December 2007.

CERT Coordination Center (2007), The Use of Malware Analysis in Support of Law Enforcement, *www.securitynewsportal.com/securitynews/article.php?title=The_Use_of_Malware_Analysis_in_Support_of_Law_Enforcement*, last accessed 11 December 2007.

Charney, S. (2005), "Combating Cybercrime: A Public-Private Strategy in the Digital Environment", Microsoft Corporation, www.nwacc.org/programs/conf05/UNCrimeCongressPaper.doc, last accessed 11 December 2007.

Chen, P.-Y., G. Kataria and R. Krishnan (2005) "Software Diversity for Information Security", Fourth Workshop on the Economics of Information Security, Harvard University, http://infosecon.net/workshop/pdf/47.pdf.

Choi, J. P., C. Fershtman and N. Gandal (2005), "Internet Security, Vulnerability Disclosure, and Software Provision", Fourth Workshop on the Economics of Information Security, Harvard University, http://infosecon.net/workshop/pdf/9.pdf.

Clayton, R. (2007), "Phishing and the gaining of 'clue'", Light Blue Touchpaper, www.lightbluetouchpaper.org/2007/08/16/phishing-and-the-gaining-of-clue/.

Computer Economics (2007), 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code, *www.computereconomics.com/page.cfm?name=Malware%20Report*.

Congressional Budget Office Cost Estimate (2007), "H.R. 1525 Internet Spyware (I-SPY) Prevention Act of 2007", as ordered reported by the House Committee on the Judiciary, 7 May, *www.cbo.gov/ftpdocs/80xx/doc8076/hr1525.pdf*.

Consumer Reports WebWatch (2005), "Leap of Faith: Using the Internet Despite the Dangers", results of a National Survey of Internet Users for Consumer Reports WebWatch, www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm ;

Consumers Union (2007), "State of the 'Net' Survey '07", *Consumer Reports*, 2007(9): 28-34.

Consumentenbond (2006), "PC beveiliging & veilig Internet: Een enquête onder computergebruikers", *Consumentengids*, 2006(11).

Council of Europe (2001), *Convention on Cybercrime*, Budapest, 23 November, *http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm*.

Council of Europe (2007), "Status of Signatories and Parties to the Convention on Cybercrime", CETS No. 185, *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/04&CL=ENG*, last accessed 11 December 2007.

Counterpane & MessageLabs (2006), *2005 Attack Trends & Analysis*, *www.counterpane.com/dl/attack-trends-2005-messagelabs.pdf*.

CSI (Computer Security Institute) (2007), *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey*, *www.gocsi.com/forms/csi_survey.jhtml*.

CSI/FBI Computer Crime and Security Survey (2006), *www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=4SCJQ3Y0PCPTOQSNDLPCKHSCJUNN2JVN*.

Dancho D. (2006), "Malware – future trends", *www.linuxsecurity.com/docs/malware-trends.pdf*, last accessed 7 December 2007.

Dearne, K. (2007), "Online security begins at home", *Australian IT News*, *http://australianit.news.com.au/articles/0,7204,21675098%5E24169%5E%5Enbv%5E,00.html*, last accessed 11 December 2007.

Denning, D. (2000), "Statement by Dorothy E. Denning", Georgetown University, *http://ftp.fas.org/irp/congress/2000_hr/00-05-23denning.htm*.

Devillard, A. (2006), *Le « phishing » en France, peu de victimes mais une menace grandissante*, 01net, *www.01net.com/editorial/311785/cybercriminalite/le-phishing-en-france-peu-de-victimes-mais-une-menace-grandissante/*, last accessed 11 December 2007.

Dhamija, Rachna, *et al.* (2007), "The Emperor's New Security Indicators, An evaluation of website authentication and the effect of role playing on usability", *http://usablesecurity.org/emperor*.

Dot-TK (2007), "Dot Tk Free Domain Names – A New Approach To Make A Whole Top Level Country Domain Free Of Illicit Content", *www.dot.tk/en/press_jul16-07.pdf*.

Du, Y. (2007), "Introduction of malware Issues", presentation by CNCERT/CC at the APEC-OECD Malware Workshop, *www.oecd.org/dataoecd/33/59/38653107.pdf*, last accessed 10 December, 2007.

Dynes, S., E. Andrijicic and M. E. Johnson (2006), "Costs to the U.E. Economy of Information Infrastructure Failure from Field Studies and Economic Data", Fifth Workshop on the Economics of Information Security 2006, *http://weis2006.econinfosec.org/docs/4.pdf*.

Dynes, S., H. Brechbühl and M. E. Johnson (2005), *Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm*, Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/51.pdf*.

The Economist (2007), "A cyber riot", 10 May, *www.economist.com/world/europe/displaystory.cfm?story_id=9163598*, accessed 4 December, 2007.

Edwards, L., (2004), "Reconstruction Consumer Privacy Protection Online", *International Review of Law – Computers & Technology*, Vol. 18, No. 3, p. 315.

Eeten, M. J. van and J. M. Bauer (2008), "Economics of Malware: Security Decisions, Incentives and Externalities", *OECD Science, Technology and Industry Working Papers*, 2008/1, OECD Publishing, doi:10.1787/241440230621.

Ehrlich, I. (1996), "Crime, Punishment, and the Market for Offenses", *The Journal of Economic Perspectives*, 10(1): 43-67, *http://links.jstor.org/sici?sici=0895-3309%28199624%2910%3A1%3C43%3ACPATMF%3E2.0.CO%3B2-U*.

ENISA (European Network and Information Security Agency) (2006), *Provider Security Measures Part 1: Security and Anti-Spam Measures of Electronic Communication Service Providers - Survey*, *www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf*.

Ernst & Young (2007), *Global Information Security Survey 2006*, *www.ey.nl/download/publicatie/2006_GISS_EYG_AU0022.pdf*.

European Union (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities*, L 281/31, *http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf*, accessed 11 December 2007.

European Union (2002), "Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector", *Official Journal of the European Communities*, L 201/37, *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf*, accessed 11 December 2007.

European Union (2005), "Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems", *Official Journal of the European Communities,* L 69/67 *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf*.

European Commission (2007), "E-Communication Household Survey", Special Eurobarometer 274, Wave 66.3, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_274_en.pdf*, last accessed 10 December 2007.

Fox, J. (2007), *Consumer Reports: Putting Consumers Back in Control*, Federal Trade Commission, *www.ftc.gov/bcp/workshops/spamsummit/presentations/Consumers.pdf*.

Franklin, J., *et al*. (2007), "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants", CCS'07, *www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf*.

Friedman, L. S. (2002), *The Microeconomics of Public Policy Analysis*, Princeton University Press, Princeton.

F-Secure (2007), "IT Security Threat Summary for H1 2007", F-Security Data Security Wrapup 1/2007, *www.f-secure.com/2007/1/*.

Gal-Or, E. and A. Ghose (2003), "The Economic Consequences of Sharing Security Information", 2nd Annual Workshop on Economics and Information Security, *www.cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf*.

Gal-Or, E. and A. Ghose (2005), "The Economic Incentives for Sharing Security Information", *Information Systems Research*, 16(2): 186-208, *www.andrew.cmu.edu/user/aghose/Infosec.pdf*.

Gartner (2005), "Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce", press release, *www.gartner.com/press_releases/asset_129754_11.html*.

Gaudin, S. (2007), "T.J. Maxx Security Breach Costs Soar To 10 Times Earlier Estimate", *Information Week*, *http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201800259*.

GetSafeOnline (2006), *The Get Safe Online Report*, October, *www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf*.

Google, Inc. (2007), "The Ghost In The Browser Analysis of Web-based Malware", *www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf*, accessed 12 December 2007.

Gordon, L. A. and M. P. Loeb (2002), "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, Vol. 5, Issue 4, pp. 438-457, *http://portal.acm.org/citation.cfm?id=581274*.

Govcert.nl (2006), *Annual Review, www.govcert.nl/render.html?it=147*, last accessed 13 December 2007.

Govcert.nl (2007), "Botnets", presentation given by Douwe Leguit at the APEC-OECD Malware Workshop, *www.oecd.org/dataoecd/34/36/38653287.pdf*, accessed 10 December 2007.

Greene, T. (2007), "Kapersky seeks help from international police to fight cybercrime", *Network World*, *www.networkworld.com/news/2007/013107-kaspersky-cybercrime.html*, accessed 14 December 2007.

Heidrich, J. (2007), "IP-Blacklisting zur Spam-Abwehr kann rechtswidrig sein", *Heise Online, www.heise.de/newsticker/meldung/97568*.

Higgins, K. J. (2007a), "Battling Bots, Doing No Harm", *Dark Reading*, *www.darkreading.com/document.asp?doc_id=118739*.

Higgins, K. J. (2007b), "Untying the Bot Knot", *Dark Reading*, *www.darkreading.com/document.asp?doc_id=114081&WT.svl=news1_6*

Honeynet Project and Research Alliance (2007), *Know your enemy: Fast-Flux Service Networks*, *www.honeynet.org/papers/ff/*, accessed 13 December, 2007.

House of Lords (2007a), *Science and Technology Committee, 5th Report of Session 2006–07, Personal Internet Security, Volume I: Report*, Authority of the House of Lords, *www.publications.parliament.uk/pa/ld/ldsctech.htm*.

House of Lords (2007b), *Science and Technology Committee, 5th Report of Session 2006–07, Personal Internet Security, Volume II: Evidence*, Authority of the House of Lords, *www.publications.parliament.uk/pa/ld/ldsctech.htm*.

Hypponen, M. (2006); "Malware goes mobile"; *Scientific American,* pp.70-77, *www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf*, accessed 13 December 2007.

iGillottResearch, Inc. (2006), "The Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks", White Paper, September, *www.trustedcomputinggroup.org/groups/mobile/Final_iGR_mobile_security_white_paper_sept_2006.pdf*, accessed 7 December 2007.

ITU (International Telecommunications Union) (2007), "Executive Summary", *World Information Society Report 2007: Beyond WSIS*, *www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07-summary.pdf*.

Javelin Strategy & Research (2007), *2007 Identity Fraud Survey Report – Consumer Version How Consumers Can Protect Themselves, www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf*, accessed 14 December 2007.

Just, R. E., D. L. Hueth and A. Schmitz (2004), *The Welfare Economics of Public Policy: A Practical Approach to Project and Policy Evaluation*, Edward Elgar, Cheltenham, UK and Northampton, MA.

Kaspersky Labs (2006), *Malware Evolution 2006: Executive Summary*, *www.kaspersky.com/malware_evolution_2006_summary*.

Krebs, B. (2006), "The New Face of Phishing", Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html.*

Krebs, B. (2007), "Study: $3.2 Billion Lost to Phishing in 2007", Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2007/12/study_32_billion_lost_to_phish_1.html*.

Krebs, B. (2008), "Banks: Losses from Computer Intrusions Up in 2007", Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html*.

Kunreuther, H. and G. Heal (2003), "Interdependent security", *Journal of Risk and Uncertainty*, 26(2): 231.

Lacohée, H., S. Crane and A. Phippen (2006), "Trustguide: Final Report", BT Group Chief Technology Office, Research & Venturing / HP Labs / University of Plymouth, Network Research Group, *www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf*.

LaRose, R., N. Rifon, S. Liu and D. Lee (2005), "Understanding Online Safety Behavior: A Multivariate Model", International Communication Association, New York, *www.msu.edu/~isafety/papers/ICApanelmult21.htm*.

Lemos, R. (2006), "Attackers pass on OS, aim for drivers and apps", Security Focus website, *www.securityfocus.com/news/11404*.

Lemos, R. (2007), "Estonia gets respite from web attacks", Security Focus website, *www.securityfocus.com/brief/504*.

Liu, P.-W. (2007), "Panel Discussion: Gaps and Challenges", presentation at the OECD-APEC Tel Malware Workshop by the Director of the Information and Communication Security Technology Center, Chinese Taipei, *www.oecd.org/dataoecd/34/19/38653499.pdf*, accessed 10 December 2007.

McAfee, Inc. (2006), "Virtual Criminology Report 2007 Organized Crime and the Internet", *McAfee Avert® Labs Technical White Papers,* December, *www.mcafee.com/us/threat_center/white_paper.html*.

McAfee Inc. (2007), "Identity Theft", *McAfee Avert® Labs Technical White Papers*, January, *www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf*.

McCarthy, C. (2007), "Study: Identity theft keeps climbing", *Cnet News*, *http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html*.

McNamara, P. (2007), "Survey: Identity theft on the decline", *Network World*, *www.networkworld.com/community/?q=node/11009*, accessed 11 December 2007.

Marshall, A. (1920), *Principles of Economics: An Introductory Volume*, Macmillan, London.

Mashevsky, Y. (2007), "The Virtual Conflict – Who Will Triumph?", *The Virtualist*, *www.viruslist.com/en/analysis?pubid=204791915*.

Mell, P., K. Kent and J. Nusbaum (2005), *Guide to Malware Incident Prevention and Handling*, National Institute of Standards and Technology, *http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf*.

Messaging Anti-Abuse Working Group (2007), "Email Metrics Program: The Network Operators' Perspective; Report #5 - First Quarter 2007, June 2007", *www.maawg.org/about/MAAWG20071Q_Metrics_Report.pdf*, accessed 10 December 2007.

NISCC (UK National Infrastructure Security Information Centre) (2005), "Targeted TrojanEmail Attacks", *NISCC Briefing*, 08/2005, *www.cpni.gov.uk/docs/ttea.pdf*, accessed 7 December 2007.

MessageLabs (2006), *MessageLabs Intelligence: 2006 Annual Security Report - A Year of Spamming Dangerously: The Personal Approach to Attacking, www.messagelabs.com/mlireport/2006_annual_security_report_5.pdf*, accessed 10 December 2007.

Messagelabs (2007), *MessageLabs Intelligence: 2007 Annual Security Report - A year of storms, spam and socializing, www.messagelabs.com/resources/mlireports*, accessed 10 December 2007.

Messmer, E. and D. Pappalardo (2005), "Extortion via DDoS on the rise: Criminals are using the attacks to extort money from victimized companies", *Computerworld*, *www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html*, accessed 7 December 2007.

Microsoft (2005), *The Trustworthy Computing Security Development Lifecycle*, *http://msdn2.microsoft.com/en-us/library/ms995349.aspx*.

Microsoft (2006a), *Security Intelligence Report (January – June 2006)*, *www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en*.

Microsoft (2006b), *Security Intelligence Report (July - December 2006), www.microsoft.com/downloads/details.aspx?familyid=af816e28-533f-4970-9a49-e35dc3f26cfe&displaylang=en*, accessed 3 December 2007.

Microsoft (2007), "Storm Drain", Anti-Malware Engineering Team Weblog, *http://blogs.technet.com/antimalware/archive/2007/09/20/storm-drain.aspx*.

Netcraft Toolbar Community (2007), "Phishing By The Numbers: 609,000 Blocked Sites in 2006", Netcraft website, *http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html*, accessed 11 December 2007.

NIST (National Institute of Standards and Technology) (2005), *Guide to Malware and Incident Handling: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-83, November, *http://csrc.nist.gov/publications/nistpubs/800-83/SP800 83.pdf*.

NIST (2008), *Computer Security Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-61 Revision 1, March, *http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf*.

Nowotny, E. (1987), *Der öffentliche Sektor: Einführung in die Finanzwissenschaft*, Springer, Berlin.

Oberoi, S. (2007), "Addressing the Malware Problem", presentation given at the APEC-OECD Malware Workshop, *http://www.oecd.org/dataoecd/33/57/38653049.pdf*.

OECD (2002a), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, *www.oecd.org/dataoecd/16/22/15582260.pdf*.

OECD (2002b). "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security – Questions and Answers", *www.oecd.org/dataoecd/27/6/2494779.pdf*.

OECD (2005a), "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2005)1/FINAL, 16 December, *www.oecd.org/dataoecd/16/27/35884541.pdf*.

OECD (2005b), *Science, Technology, and Industry Scoreboard*, 2005 edition, OECD Publishing, Paris.

OECD (2006), "OECD Anti-Spam Toolkit of Recommended Policies and Measures", report of the OECD Task Force on Spam, DSTI/CP/ICCP/SPAM(2005)3/FINAL, www.oecd-antispam.org/, accessed 13 December 2007.

OECD (2007a), *OECD Communications Outlook 2007,* Information and Communications Technologies, OECD Publishing, Paris.

OECD (2007b), "APEC-OECD Malware Workshop: Summary Record", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)15, 15 June, *www.oecd.org/dataoecd/37/60/38738890.pdf*.

OECD (2007c), "The Development of Policies for the protection of Critical Information (CII): A comparative analysis in four OECD countries: Canada, Korea, the United Kingdom and the United States", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2006)15/FINAL, 6 February, *www.olis.oecd.org/olis/2006doc.nsf/ENGREFCORPLOOK/NT00007766/$FILE/JT03221273.PDF*.

OECD (2008a), "The Development of Policies for the protection of Critical Information (CII): A comparative analysis in three OECD countries: Australia, Japan, and the Netherlands", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)16/FINAL, 9 January, *www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005A5E/$FILE/JT03238526.PDF*.

OECD (2008b), "Scoping Paper on Online Identity Theft", unclassified document, DSTI/CP(2007)3/FINAL, 15 May, *www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005CAE/$FILE/JT03240674.PDF*.

OECD (2008c), "The Development of Policies for the Protection of Critical Information Infrastructures (CII): A Comparative Analysis in Seven OECD Countries: Australia, Canada, Korea, Japan, The Netherlands, The United Kingdom and the United States", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)20/FINAL, 8 April, *http://www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005A8A/$FILE/JT03243745.PDF*.

ORF (2007), *Spamhaus antwortet auf nic.at*. futurezone, *http://futurezone.orf.at/it/stories/201738/*, accessed 25 November 2007.

Outlaw.com (2007), "Phishing attack evades ABN Amro's two-factor authentication", OUT-LAW News, 18 April, *www.out-law.com/page-7967*, accessed 11 December 2007.

PayPal (2007), "Key Financial Facts", Paypal website, *www.pppress.co.uk/* .

Pigou, A. C. (1932), *The Economics of Welfare*, Macmillan, London.

Poindexter, J. C., J. B. Earp and D. L. Baumer (2006), "An experimental economics approach toward quantifying online privacy choices", *Information Systems Frontiers*, 8(5): 363-374.

Poulsen, Kevin (2003), *Slammer worm crashed Ohio nuke plant network,* Security Focus, *www.securityfocus.com/news/6767*, accessed 11 December 2007.

Register (2007), "Phishing attack evades bank's two-factor authentication", *www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/*.

Rescorla, E. (2004), "Is finding security holes a good idea?", Workshop on Economics and Information Security 2004, *www.rtfm.com/bugrate.pdf*.

Rifon, N., E. T. Quilliam and R. LaRose (2005), "Consumer Perceptions of Online Safety", paper presented at the International Communication Association, Communication and Technology Division, New York, 27 May, *www.msu.edu/~isafety/papers/ICApanelfg.htm*.

Rowe, B. R. and M. P. Gallaher (2006), "Private Sector Cyber Security Investment: An Empirical Analysis", Fifth Workshop on the Economics of Information Security, Cambridge, March, *www.weis2006.econinfosec.org/docs/18.pdf*.

RSA Security (2006), "Internet Confidence Index Shows that – for Businesses and Consumers – Transactions are Outpacing Trust", *www.rsa.com/press_release.aspx?id=6502,* accessed 14 December 2007.

Schechter, S. E. (2004), *Computer Security Strength & Risk: A Quantitative Approach*, thesis presented to the Division of Engineering and Applied Sciences, Harvard University, May, *www.eecs.harvard.edu/~stuart/papers/thesis.pdf*.

Schneier, B. (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley, New York.

Schneier, B. (2005), "A Real Remedy for Phishers", *Wired News*, *www.wired.com/news/politics/0,1283,69076,00.html*.

Schneier, B. (2007), "Information Security and Externalities", NSF/OECD Workshop on Social & Economic Factors Shaping The Future of the Internet, Washington, DC, *www.oecd.org/dataoecd/60/8/37985707.pdf*.

Shifrin, T. (2007), "Lose an unencrypted laptop and 'face criminal action'", *Computerworld UK*, 15 November, *www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=6241*.

Shin, A. (2007a); "Is Identity Theft Decreasing?", The Checkout Washington Post Blog, 6 February, *http://blog.washingtonpost.com/thecheckout/2007/02/is_identity_theft_decreasing.html*.

Shin, A. (2007b), "Looking for a Job? Phishers Are Looking for You.", The Checkout Washington Post Blog, 12 February, *http://blog.washingtonpost.com/thecheckout/2007/02/looking_for_a_job_phishers_are.html*.

Shostack, A. (2005), "Avoiding Liability: An Alternative Route to More Secure Products", Fourth Workshop on the Economics of Information Security, Harvard University, *infosecon.net/workshop/pdf/44.pdf*.

Snyder, W. (2007), "Time to Deploy improvement of 25 %", Mozilla Security Blog, *http://blog.mozilla.com/security/2007/06/18/time-to-deploy-improvement-of-25-percent/*.

Sokolov, D. A. (2007), "Spamhaus.org setzt Österreichs Domainverwaltung unter Druck", Heise online, *www.heise.de/newsticker/meldung/91417*; last accessed 25 November 2007.

Sophos (2006a), "The Growing Scale of the Threat Problem", *www.sophos.com/sophos/docs/eng/papers/Growing-threat-wpus.pdf*, accessed 7 December, 2007.

Sophos (2006b), "Devious Arhiveus ransomware kidnaps data from victims' computers", *www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html*, accessed December 7, 2007.

Sophos (2006c), "Married couple formally charged over spyware Trojan horse", *www.sophos.com/pressoffice/news/articles/2006/03/israeliesp2.html*, accessed 13 December 2007.

Sophos (2007a), "Security Threat Report", Sophos Security white paper, *www.sophos.com/security/whitepapers/*, last accessed 12 December 2007.

Sophos (2007b), "Security Threat Report Update July 2007", Sophos Security white paper, *www.sophos.com/security/whitepapers/*, accessed 12 December 2007.

South, G. (2007), "Web issues over banking code", *The New Zealand Herald*, *www.nzherald.co.nz/topic/story.cfm?c_id=126&objectid=10458545*.

Spamhaus (2007), "Report on the criminal 'Rock Phish' domains registered at Nic.at", Spamhaus statements, 21 June, *www.spamhaus.org/organization/statement.lasso?ref=7*, accessed 25 November 2007.

Table of Contents

Executive Summary 11

Background.....15

Part I. The Scope of Malware 19

Chapter 1. **An Overview of Malware**.....21

What is malware?.....21
How does malware work? 23
Malware on mobile devices.....27
The Malware Internet: botnets 27
What are botnets used for?.....30
Botnets Command and Control (C&C) models 30
Botnet figures.....31
Botnets and broadband.....33
Spam and botnets 33
The role of blacklists in combating botnets.....35

Chapter 2. **Malware Attacks: Why, When and How?** 41

Types of malware attacks.....41
Indirect attacks on the DNS 43
Attacks that modify data 44
Attacks on identity 45
Attacks on single and multi-factor authentication.....46
Attacks on digital certificates and secure socket layer (SSL) 47
Why attacks are perpetrated 48
Malware attack trends 52
Origin of malware attacks 53
The malicious actors 54
The malware business model 56

Chapter 3. **Malware: Why Should We Be Concerned? 65**

Malware-enabling factors.....65
The costs of malware 67
Challenges to fighting malware.....74

Part II. The Economics of Malware.....79

Chapter 4. **Cybersecurity and Economic Incentives 81**

Increased focus on incentive structures.....82
The economic perspective.....84

Chapter 5. **Survey of Market Participants: What Drives Their Security Decisions?.....89**

Internet service providers 89
E-commerce companies 103
Software vendors.....109
Domain registrars 122
End users 129

Annex 5.A1. List of Interviewees 137

Chapter 6. **The Market Consequences of Cybersecurity: Defining Externalities and Ways to Address Them 139**

Three major categories of externalities 139
Distributional and efficiency effects 143
Survey results on the costs of malware 145
Key findings 146

Part III. Malware: What Can Be Done? 149

Chapter 7. **The Role of End Users, Business and Government.....151**

Key participants 151
Incentives and disincentives – Highlights from Part II 152
The impact on society at large.....155

Chapter 8. **What Is Already Being Done?.....157**

Summary of key efforts.....157
Instruments, structures and initiatives that address malware 159

Chapter 9. **Possible Next Steps.....183**

A global partnership against malware 183
Areas for improvement and further exploration.....184
Conclusion 192

Annex A. Background Data on Malware 195

Annex B. Research Design for Economics of Malware.....209

Annex C. A Framework for Studying the Economics of Malware ..213

Glossary of Malware Terms 227

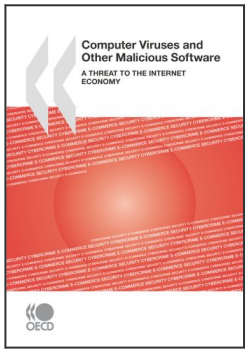
Bibliography 231

Figures

1.1 US-CERT incident reporting trends 24
1.2 Top five malware (2007).....25
1.3 The botnet lifecycle 29
1.4 Command and control for botnets 31
2.1 Online ID theft attack system involving malware 51
2.2 General attack trends.....52
2.3 Malicious actors 54
2.4 Visibility of malware vs. malicious intent.....56
2.5 Self sustaining attack system using malware 58
8.1 Botnet infection rate of Korea (2005-2006) 175
A.1 Online ID theft trojan incidents handled by AusCERT.....196
A.2 Total artefacts by month.....198
A.3 New artefacts per month.....198
A.4 CERT-FI Abuse Autoreporter monthly case processing volume 199
A.5 Incident reporting to KrCERT/CC by month (2005-2006) 200
A.6 Information gathered from KrCERTr honeynets.....200
A.7 Incidents handles by NorCERT in 2007.....201
A.8 Trojan incidents targeting UK banks.....202
A.9 Increase in the number of new malicious programmes 202
A.10 Microsoft malicious software activity 203
A.11 Trojans verses Windows Worms and Viruses in 2006.....204
A.12 Malicious code types by volume 205
C.1 Information industry value net.....214
C.2 Markets for crime and security 216
C.3 Markets for crime and security 217
C.4 Externalities with reputation.....225

Boxes

1.1 Malware: a brief history 22
1.2 Examples of malware propagation vectors 26
1.3 The Dutch botnet case 32
1.4 FTC v. Dugger 35
2.1 The Estonian case 42
2.2 A closer look at DNS 44
2.3 The two-factor token attack 47
2.4 The problem with digital certificates and SSL 48
2.5 A ransom example: the Arhiveus 49
2.6 The case of Michael and Ruth Haephrati 50
4.1 OECD Guidelines and the economics of cybersecurity 83
4.2 The problem with prevailing research methods 86
5.1 Microsoft's Vista: an attempt to balance compatibility and security 118
7.1 Different types of incentives 153
A.1 Summary of sample data on malware 206



From:

Computer Viruses and Other Malicious Software

A Threat to the Internet Economy

Access the complete publication at:

https://doi.org/10.1787/9789264056510-en

Please cite this chapter as:

OECD (2009), "Executive Summary - Background", in *Computer Viruses and Other Malicious Software: A Threat to the Internet Economy*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264056510-2-en

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at http://www.oecd.org/termsandconditions.